EDIMAX

NETWORKING PEOPLE TOGETHER

ES-5240G+
24-Port GbE Web Smart Switch

User's Manual

Version 1.0 / June 2007

COPYRIGHT

Table of Contents

Caution

Circuit devices are sensitive to static electricity, which can damage their delicate electronics. Dry weather conditions or walking across a carpeted floor may cause you to acquire a static electrical charge.

To protect your device, always:

- Touch the metal chassis of your computer to ground the static electrical charge before you pick up the circuit device.
- Pick up the device by holding it on the left and right edges only.

Electronic Emission Notices

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a class A computing device pursuant to Subpart J of part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment.

European Community (CE) Electromagnetic Compatibility Directive

This equipment has been tested and found to comply with the protection requirements of European Emission Standard EN55022/EN60555-2 and the Generic European Immunity Standard EN50082-1.

EMC:	EN55022(1988)/CISPR-22(1985)	class A
	EN60555-2(1995)	class A
	EN60555-3	
	IEC1000-4-2(1995)	4K V CD, 8KV, AD
	IEC1000-4-3(1995)	3V/m
	IEC1000-4-4(1995)	1KV – (power line), 0.5KV – (signal line)

1. Introduction

1-1. Overview of 24-Port GbE Web Smart Switch

24-port Gigabit Web Smart Switch is a standalone switch that meets IEEE 802.3/u/x/z standards. The switch is equipped with included 20 x 10/100/1000Mbps TP port and 4 x Gigabit TP/SFP Fiber auto-sense port Web Smart management Ethernet Switch. The switch is designed to incorporate a Web-based management unit that allows the network administrator to access the switch to monitor, configure and control the activity of each port. In addition, the switch implements the QoS (Quality of Service), VLAN, and Trunking features. It is suitable and optimized for office applications.

Port 21, 22, 23 and 24 are designed to support two types of connectors --- TP and SFP Fiber (LC, BiDi-SC…). Each of these ports supports 10/100/1000Mbps TP or 1000Mbps SFP Fiber with auto-sense function. The 1000Mbps SFP Fiber transceiver is used for high-speed connected expansion.

- 1000Mbps LC, Multi-Mode, SFP Fiber transceiver
- 1000Mbps LC, 10km, SFP Fiber transceiver
- 1000Mbps LC, 30km, SFP Fiber transceiver
- 1000Mbps LC, 50km, SFP Fiber transceiver
- 1000Mbps BiDi-SC, 20km, 1550nm SFP Fiber WDM transceiver
- 1000Mbps BiDi-SC, 20km, 1310nm SFP Fiber WDM transceiver

The 10/100/1000Mbps TP is a standard Ethernet port that meets IEEE 802.3/u/x/z standards. The 1000Mbps SFP Fiber transceiver is a Gigabit Ethernet port that fully complies with all IEEE 802.3z and 1000Base-SX/LX standards.

1000Mbps Single Fiber WDM (BiDi) transceiver is designed with an optic Wavelength Division Multiplexing (WDM) technology that transports bi-directional full duplex signal over a single fiber simultaneously.

• Key Features in the Device

QoS:

Supports 802.1p VLAN tag priority and DSCP in Layer 3 network framework

VLAN:

Supports Port-based VLAN, IEEE802.1Q Tag VLAN, 24 active VLANs and VLAN ID 1~4094

Port Trunking:

Allows one or more links to be aggregated together to form a Link Aggregation Group by the static setting

1-2. Checklist

Before you start installing the switch, verify that the package contains the following:

- 24-Port GbE Web Smart Switch
- SFP Modules (optional)
- Mounting Accessory (for 19” Rack Shelf)
- CD-ROM with User's Manual
- Power Adapter

Please notify your sales representative immediately if any of the aforementioned items is missing or damaged.

1-3. Features

The 24-Port GbE Web Smart Switch is a standalone off-the-shelf switch. It securely serves your network and efficiently provides comprehensive features for the users to perform system network administration as listed below.

• Hardware

- 20 10/100/1000Mbps Auto-negotiation Gigabit Ethernet TP ports
- 4 10/100/1000Mbps TP or 1000Mbps SFP Fiber dual media auto sense
- 400KB on-chip frame buffer
- Jumbo frame support
- Programmable classifier for QoS (Layer 2/Layer 3)
- 8K MAC address and support VLAN ID (1~4094)
- Per-port shaping, policing, and Broadcast Storm Control
- IEEE802.1Q-in-Q VLAN support
- Full-duplex flow control (IEEE802.3x) and half-duplex backpressure
- Extensive front-panel diagnostic LEDs; System: Power, TP Port1-24: LINK/ACT, 10/100/1000Mbps, SFP Port 21, 22, 23,24: SFP(LINK/ACT)

• Management

- Supports concisely the status of port and easily port configuration
- Supports per port traffic monitoring counters
- Supports a snapshot of the system information when you login
- Supports port mirror function
- Supports the static trunk function
- Supports 802.1Q VLAN
- Supports user management and limits one user to login
- Maximal packet length can be up to 9600 bytes for jumbo frame application
- Supports Broadcasting Suppression to avoid network suspended or crashed

- Supports to send the trap event while monitored events happened
- Supports default configuration which can be restored to overwrite the current configuration which is working on via Web UI and Reset button of the switch
- Supports hot swap plug/unplug SFP modules
- Supports Quality of Service (QoS) for real time applications based on the information taken from Layer 2 to Layer 3.
- Built-in web-based management instead of using CLI interface, providing a more convenient GUI for the user

1-4. View of 24-Port GbE Web Smart Switch

Fig. 1-1 Full View of 24-PORT GBE WEB SMART SWITCH

1-4-1. User Interfaces on the Front Panel (Button, LEDs and Plugs)

There are 24 TP Gigabit Ethernet ports and 4 SFP fiber ports for optional removable modules on the front panel of the switch. LED display area. Locating on the left side of the panel, Power LED, which indicates the power status and 24 ports working status of the switch.

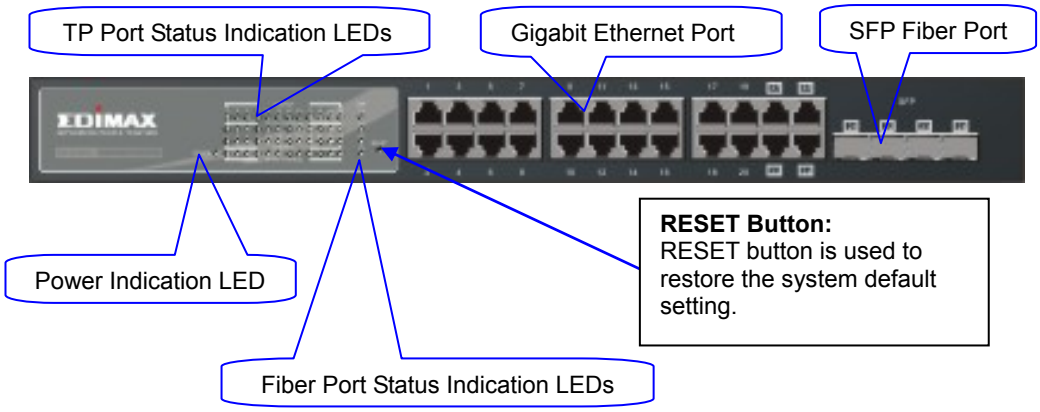


Fig. 1-2 Front View of 24-PORT GBE WEB SMART

• **LED Indicators**

LED	Color	Function
System LED		
POWER	Green	Lit when +3.3V power is coming up
10/100/1000Ethernet TP Port 1 to 24 LED		
LINK/ACT	Green	Lit when connection with remote device is good Blinks when any traffic is present
10/100/1000Mbps	Green/ Amber	Lit Green when TP link on 1000Mbps speed Lit Amber when TP link on 100Mbps speed Off when 10Mbps or no link occur Blinks when any traffic is present
1000SX/LX Gigabit Fiber Port 21, 22, 23, 24 LED		
SFP(LINK/ACT)	Green	Lit when SFP connection with remote device is good Blinks when any traffic is present

Table1-ES-5240G+ LED Indicators table

1-4-2. User Interfaces on the Rear Panel

Fig. 1-3 Rear View of 24-PORT GBE WEB SMART SWITCH

1-5. View of the Optional Modules

Port 21~24 on this switch support two types of media --- TP and SFP Fiber (LC, BiDi-SC…); this port supports 10/100/1000Mbps TP or 1000Mbps SFP Fiber with auto-detected function. 1000Mbps SFP Fiber transceiver is used for high-speed connection expansion; nine optional SFP types provided for the switch are listed below:

- 1000Mbps LC, MM, SFP Fiber transceiver
- 1000Mbps LC, SM 10km, SFP Fiber transceiver
- 1000Mbps LC, SM 30km, SFP Fiber transceiver
- 1000Mbps LC, SM 50km, SFP Fiber transceiver
- 1000Mbps LC, SM 70km, SFP Fiber transceiver
- 1000Mbps LC, SM 110km, SFP Fiber transceiver
- 1000Mbps BiDi SC, type 1, SM 20km, SFP Fiber WDM transceiver
- 1000Mbps BiDi SC, type 2, SM 20km, SFP Fiber WDM transceiver
- 1000Mbps LC, SM 10km, SFP Fiber transceiver with DDM

Fig. 1-4 Front View of 1000Base-SX/LX LC, SFP Fiber Transceiver

Fig. 1-5 Front View of 1000Base-LX BiDi SC SFP Fiber Transceiver

2. Installation

2-1. Starting 24-Port GbE Web Smart Switch Up

This section will give users a quick start for:

- Hardware and Cable Installation
- Management Station Installation
- Software booting and configuration

2-1-1. Hardware and Cable Installation

At the beginning, please do first:

→Wear a grounding device to avoid the damage from electrostatic discharge. Be sure that power switch is OFF before you plug in AC power source

→Installing Optional SFP Fiber Transceivers to the 24-Port GbE Web Smart Switch

Note: If you do not have modules, please skip this section.

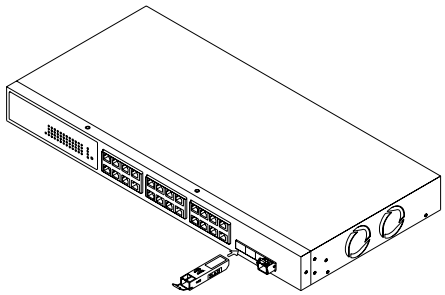


Fig. 2-1 Installation of Optional SFP Fiber Transceiver

• Connecting the SFP Module to the Chassis:

The optional SFP modules are hot swappable, so you can plug or unplug them before or while the power is turn on

1. Verify that the SFP module is the right model and conform to the chassis
2. Slide the module along the slot. Also be sure that the module is properly seated on the slot socket/connector
3. Install the media cable for network connection
4. Repeat the above steps, as needed, for each module to be installed into slot(s)
5. Turn the power ON after the above procedures are done

- **TP Port and Cable Installation**

⇒ In the switch, TP port supports MDI/MDI-X auto-crossover, so both types of cable, straight-through (Cable pin-outs for RJ-45 jack 1, 2, 3, 6 to 1, 2, 3, 6 in 10/100M TP; 1, 2, 3, 4, 5, 6, 7, 8 to 1, 2, 3, 4, 5, 6, 7, 8 in Gigabit TP) and crossed-over (Cable pin-outs for RJ-45 jack 1, 2, 3, 6 to 3, 6, 1, 2) can be used.

⇒ Use Cat. 5 grade RJ-45 TP cable to connect to a TP port of the switch. Connect the other end to a network-aware device, such as a workstation or a server.

⇒ Repeat the above steps as needed, for each RJ-45 port to be connected to a Gigabit 10/100/1000 TP device.

The switch is now in operation.

• Power On

The switch supports 100-240 VAC, 50-60 Hz power sources.The power supply will automatically convert the local AC power source to DC power. After the power is on, all LED indicators will flash once except the power LED which will stay on. This represents a reset of the system.

• Firmware Loading

Once reset, the bootloader will load the firmware into the memory. It will take about 30 seconds. Once firmware loading is finished the switch will flash all LEDs once and automatically perform a self test and then in ready state.

2-1-2. Cabling Requirements

To help ensure a successful installation and optimize the network performance, please carefully follow the cabling requirements. Using cables under the requirement.

2-1-2-1. Cabling Requirements for TP Ports

⇒ For Fast Ethernet TP network connection
— The grade of the cable must be Cat. 5 or Cat. 5e with a maximum length of 100 meters.

⇒ Gigabit Ethernet TP network connection
— The grade of the cable must be Cat. 5 or Cat. 5e with a maximum length of 100 meters. Cat. 5e is recommended.

2-1-2-2. Cabling Requirements for 1000SX/LX SFP Module

It is more complex and comprehensive contrast to TP cabling in the fiber media. Basically, there are two categories of fiber, multi mode (MM) and single mode (SM). The later is categorized into several classes by the distance it supports. They are SX, LX, LHX, XD, and ZX. From the viewpoint of connector type, there are mainly LC and BIDI SC.

— Gigabit Fiber with multi-mode LC SFP module

— Gigabit Fiber with single-mode LC SFP module

— Gigabit Fiber with BiDi SC 1310nm SFP module

— Gigabit Fiber with BiDi SC 1550nm SFP module

The following table lists the types of fiber that we support and those else not listed here are available upon request.

<table>
<tr><td rowspan="4">IEEE 802.3z Gigabit Ethernet 1000SX 850nm</td><td colspan="4">Multi-mode Fiber Cable and Modal Bandwidth</td></tr>
<tr><td colspan="2">Multi-mode 62.5/125μm</td><td colspan="2">Multi-mode 50/125μm</td></tr>
<tr><td>Modal Bandwidth</td><td>Distance</td><td>Modal Bandwidth</td><td>Distance</td></tr>
<tr><td>160MHz-Km</td><td>220m</td><td>400MHz-Km</td><td>500m</td></tr>
<tr><td>1000Base-LX/LHX/XD/ZX</td><td colspan="4">200MHz-Km 275m 500MHz-Km 550m
Single-mode Fiber 9/125μm
Single-mode transceiver 1310nm 10Km
Single-mode transceiver 1550nm 30, 50Km</td></tr>
<tr><td rowspan="4">1000Base-LX Single Fiber (BIDI SC)</td><td colspan="2" rowspan="2">Single-Mode *20Km</td><td colspan="2">TX(Transmit) 1310nm
RX(Receive) 1550nm</td></tr>
<tr><td colspan="2">Single-Mode *20Km</td><td colspan="2">TX(Transmit) 1550nm
RX(Receive) 1310nm</td></tr>
</table>

Table2-1

2-1-2-3. Switch Cascading in Topology

• Takes the Delay Time into Account

Theoretically, the switch partitions the collision domain for each port in switch cascading that you may up-link the switches unlimitedly. In practice, the network extension (cascading levels & overall diameter) must follow the constraint of the IEEE 802.3/802.3u/802.3z and other 802.1 series protocol specifications. In which the limitations are the timing requirement from physical signals defined by 802.3 series specification of Media Access Control (MAC) and PHY, and timer from some OSI layer 2 protocols such as 802.1d, 802.1q, LACP and so on.

The fiber, TP cables and devices' bit-time delay (round trip) are as follows:

<table>
<tr><th colspan="2">1000Base-X TP, Fiber</th><th colspan="2">100Base-TX TP</th><th colspan="2">100Base-FX Fiber</th></tr>
<tr><td colspan="2">Round trip Delay: 4096</td><td colspan="4">Round trip Delay: 512</td></tr>
<tr><td>Cat. 5 TP Wire:</td><td>11.12/m</td><td>Cat. 5 TP Wire:</td><td>1.12/m</td><td>Fiber Cable:</td><td>1.0/m</td></tr>
<tr><td>Fiber Cable :</td><td>10.10/m</td><td colspan="4">TP to fiber Converter: 56</td></tr>
<tr><td colspan="2">Bit Time unit : 1ns (1sec./1000 Mega bit)</td><td colspan="4">Bit Time unit: 0.01μs (1sec./100 Mega bit)</td></tr>
</table>

Table 2-2

Sum up all elements' bit-time delay, the overall bit-time delay of wires/devices must be within Round Trip Delay (bit times) in a half-duplex network segment (collision domain). For full-duplex operation, this will not be applied. You may use the TP-Fiber module to extend the TP node distance over fiber optic and provide the long haul connection.

• Typical Network Topology in Deployment

A hierarchical network with minimum levels of switch may reduce the timing delay between server and client stations. Basically, this approach will minimize the number of switches in any one path; thus lower the possibility of network loop and will improve network efficiency. If more than two switches are connected in the same network, select one switch as Level 1 switch and connect all other switches to it at Level 2. Server/Host is recommended to connect to the Level 1 switch. This is general if no VLAN or other special requirements are applied.

Case1: All switch ports are in the same local area network. Every port can access each other (See Fig. 2-2).

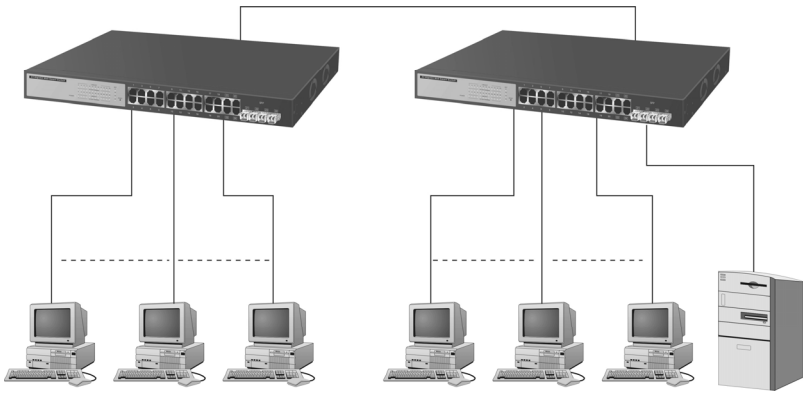


Fig. 2-2 No VLAN Configuration Diagram

If the VLAN is enabled and configured, each node in the network that can communicate each other directly is bounded to the same VLAN area.

The VLAN area is defined by which VLAN you are on. The switch supports both port-based VLAN and tag-based VLAN. They are different in practical deployment, especially in physical location. The following diagram shows how it works and what the differences are.

Case2a: Port-based VLAN (See Fig.2-3).

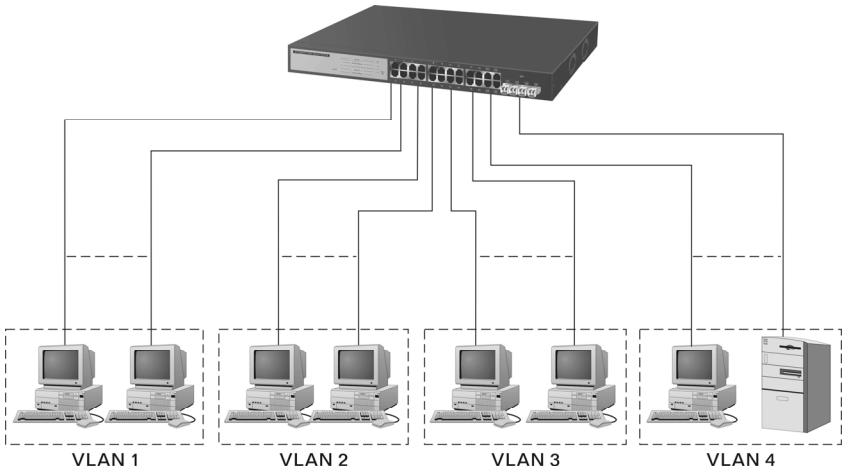


Fig. 2-3 Port-based VLAN Diagram

1. The same VLAN members can not be connected to different switches.
2. Every VLAN member can not access VLAN members from other VLAN group.
3. The network administrator has to assign different names for every VLAN group on one switch.

Case 2b: Port-based VLAN (See Fig.2-4).

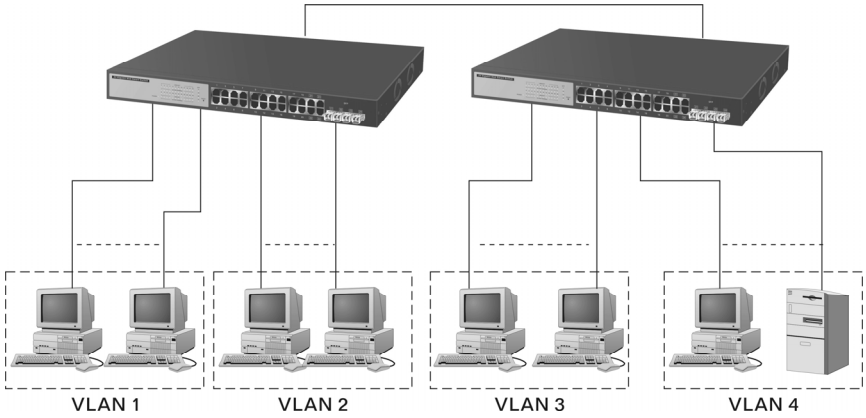


Fig. 2-4 Port-based VLAN Diagram

1. VLAN1 members can not access VLAN2, VLAN3 and VLAN4 members.
2. VLAN2 members can not access VLAN1 and VLAN3 members, but they can access VLAN4 members.
3. VLAN3 members can not access VLAN1, VLAN2 and VLAN4.
4. VLAN4 members can not access VLAN1 and VLAN3 members, but they can access VLAN2 members.

Case3a: The same VLAN members can be at different switches with the same VID (See Fig. 2-5).

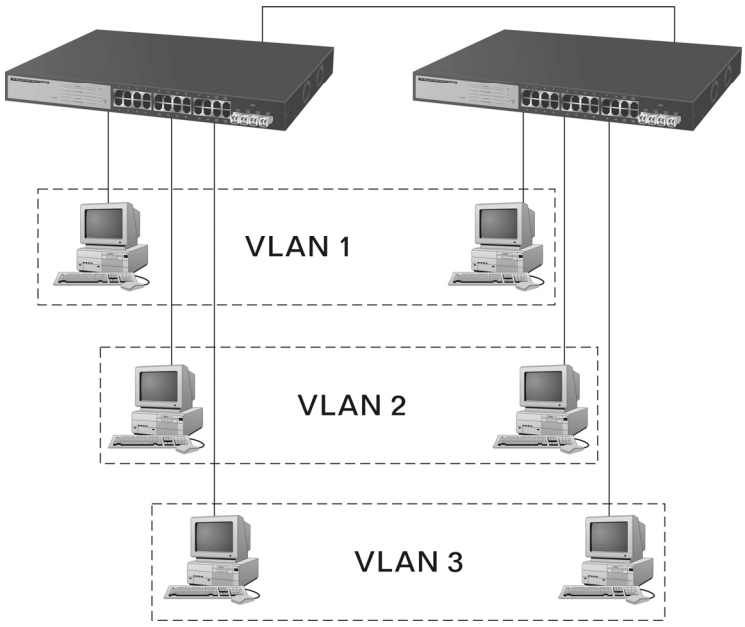


Fig. 2-5 Attribute-based VLAN Diagram

2-1-3. Configuring the Management Agent of 24-Port GbE Web Smart Switch

Just like browsing on the Internet, this switch is designed to allow users to access and manage its functions through its web-based interface. Users can monitor the status of the switch, as well as to configure the switch through this web-based interface. Here we will guide you through how to access this web based management interface.

Section 2-1-3-1: Configuring Management Agent of 24-Port GbE Web Smart Switch through Ethernet Port

2-1-3-1. Management through Ethernet Port

There are two ways to configure and monitor the switch through its Ethernet port – using a web browser and an SNMP manager program. The later one is RubyView dependant which is not covered here. Using a web browser to access the switch's web-based management UI is highly user friendly so that we will only introduce this method here.

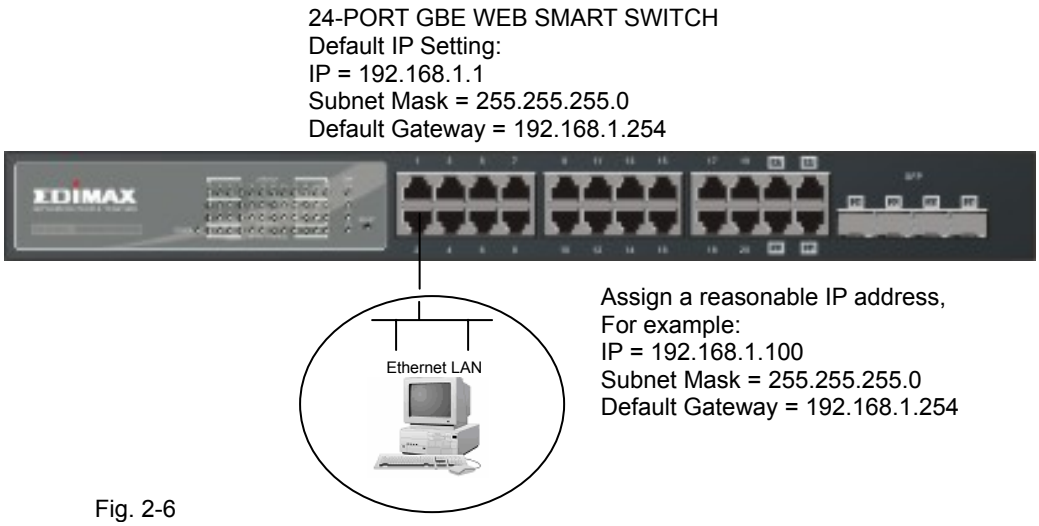


Fig. 2-6

• Managing 24-Port GbE Web Smart Switch through Ethernet Port

Before you can communicate with the switch, you should have had configured the IP address for the switch and have the IP information ready. Then, follow the procedures listed below.

1. Set up a physical path between the configured switch and a PC with a qualified UTP Cat. 5 cable with RJ-45 connectors.

   Note: If the PC directly connects to the switch, you will have to set up same subnet mask for both of them. However, the subnet mask may have to be different for the PC when it is at a remote site. Please refer to Fig. 2-6 about the 24-Port GbE Web Smart Switch default IP address information.

2. Run web browser and follow. However, the subnet mask may have to be different for the PC when it is at a remote site. Please refer to Chapter 4

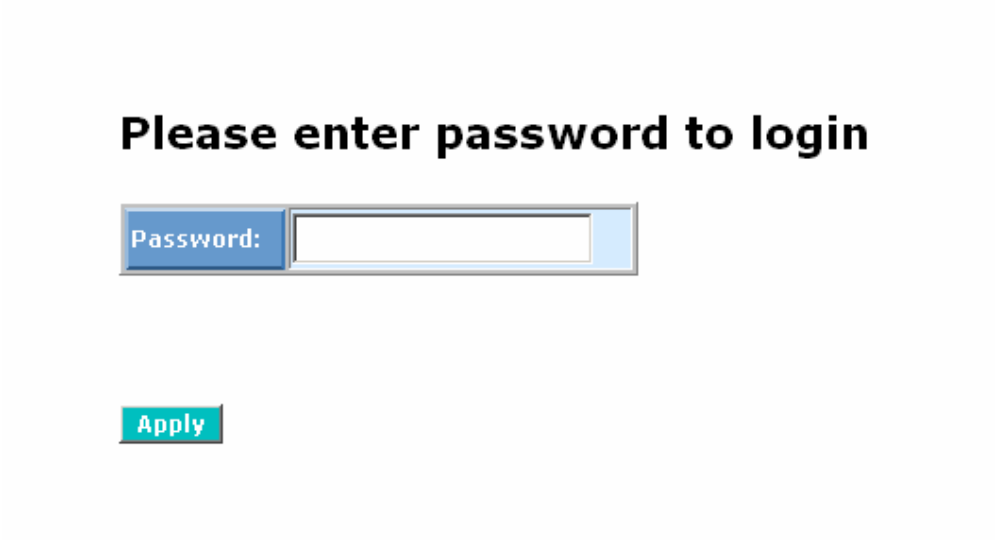


Fig. 2-7 the Login Screen for Web

2-1-4. IP Address Assignment

For IP address configuration, four parameters are required. They are IP address, Subnet Mask, Default Gateway and DNS.

IP address:

The IP address of the network device in a network is used for internetworking communication. The IP address is structured as shown in Fig. 2-8. It is classified into predefined address classes or categories.

Each class has its own network range. Each IP address comprises two parts: network identifier (address) and host identifier (address). The former indicates the network where the addressed host resides, and the latter indicates the individual host in the network which the address refers to the host identifier must be unique in the same LAN. The terms of IP address we used here is version 4, known as IPv4.

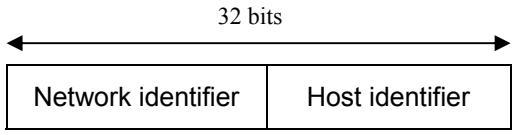
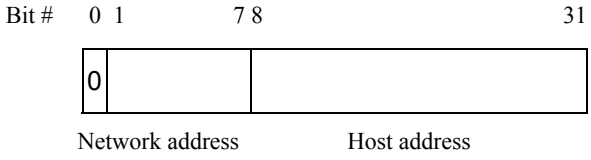


Fig. 2-8 IP address structure

According to IPv4, the IP addressed are divided three classes, class A, class B and class C. The rest of IP addresses are for multicast and broadcast. The bit length of the network prefix is the same as that of the subnet mask and is denoted as IP address/X, for example, 192.168.1.0/24. Each class has its address range as described below.

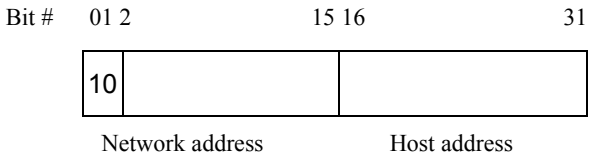
Class A:

Address is less than 126.255.255.255. There are a total of 126 networks can be defined because the address 0.0.0.0 is reserved for default route and 127.0.0.0/8 is reserved for loopback function.



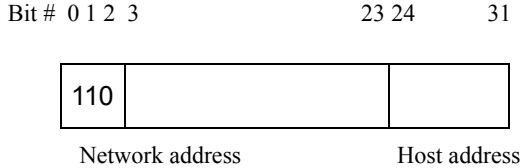
Class B:

The IP address range in between 128.0.0.0 and 191.255.255.255. Each class B network has a 16-bit network prefix followed by a 16-bit host address. There are 16,384 (2^14)/16 networks available to be defined with a maximum of 65534 (2^16 –2) hosts per network.



Class C:

The IP addresses range in between 192.0.0.0 and 223.255.255.255. Each class C network has a 24-bit network prefix followed an 8-bit host address. There are 2,097,152 (2^21)/24 networks available to be defined with a maximum of 254 (2^8 –2) hosts per network.



Class D and E:

Class D is a class with first 4 MSB (Most significance bit) set to 1-1-1-0 and is used for IP Multicast. See also RFC 1112. Class E is a class with first 4 MSB set to 1-1-1-1 and is used for IP broadcast.

According to IANA (Internet Assigned Numbers Authority), there are three specific IP address blocks reserved and to be used for extending internal network. We call them private IP addresses and they are listed below:

Class A	10.0.0.0 --- 10.255.255.255
Class B	172.16.0.0 --- 172.31.255.255
Class C	192.168.0.0 --- 192.168.255.255

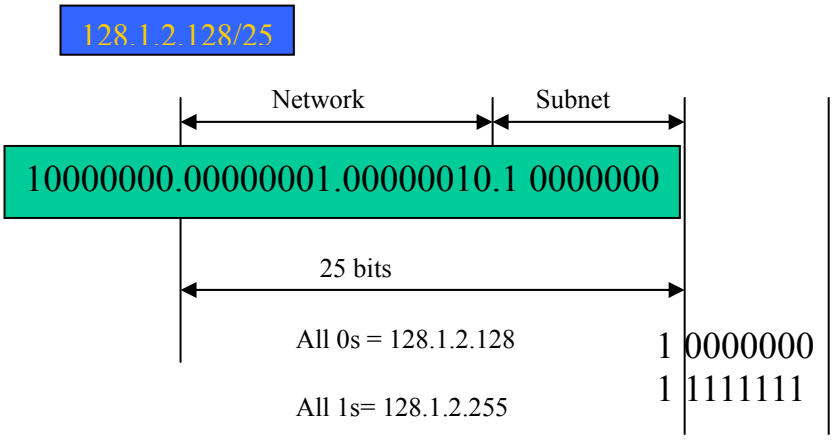
Please refer to RFC 1597 and RFC 1466 for more information.

Subnet mask:

It means the sub-division of a class-based network or a CIDR block. The subnet is used to determine how to split an IP address to the network prefix and the host address in bitwise basis. It is designed to utilize IP address more efficiently and ease the IP network management task.

For a class B network, 128.1.2.3, it may have a subnet mask 255.255.0.0 by default, in which the first two bytes are with all 1s. This means more than 60 thousands of nodes in flat IP address will be at the same network. It's too large to manage practically. Now if we divide it into smaller network by extending network prefix from 16 bits to, say 24 bits, that's using its third byte to subnet this class B network. Now it has a subnet mask 255.255.255.0, in which each bit of the first three bytes are 1s. It's now clear that the first two bytes are used to identify the class B network, the third byte is used to identify the subnet within this class B network and, of course, the last byte is the host number.

Not all IP address is available in the sub-netted network. Two special addresses are reserved. They are the ones which their host number are all zeros and all ones. or example, an IP address 128.1.2.128/25; to represent the network itself, the IP address is 128.1.2.128; and for IP broadcasting, the address used would be 128.1.2.255.



In this diagram, you can see the subnet mask with 25-bit long, 255.255.255.128, contains 126 members in the sub-netted network. Another is that the length of network prefix equals the number of the bit with 1s in that subnet mask. With this, you can easily count the number of IP addresses matched. The following table shows the result.

Prefix Length	No. of IP matched	No. of Addressable IP
/32	1	-
/31	2	-
/30	4	2
/29	8	6
/28	16	14
/27	32	30
/26	64	62
/25	128	126
/24	256	254
/23	512	510
/22	1024	1022
/21	2048	2046
/20	4096	4094
/19	8192	8190
/18	16384	16382
/17	32768	32766
/16	65536	65534

Table 2-3

There will be a maximum of 254 effective nodes exist along the sub-netted network. This network is considered to be a physical autonomous network that it owns a network IP address which may look like 168.1.2.0.

With the subnet mask, a big network can be divided into smaller pieces of network. If we want to have more than two independent networks in a worknet, a partition to the network must be performed. In this case, subnet mask must be applied.

For different network applications, the subnet mask may look like 255.255.255.240. This means it is a small network accommodating a maximum of 15 nodes in the network.

Default gateway:

When the destination of a routed packet not listed in the routing table, all traffic will be put into a device with this designated IP address, which is known as the default router. This is a routing policy.

For assigning an IP address to the switch, you need to check what the IP address of the network will be connected to the switch. Use the same network address and append your host address to it.

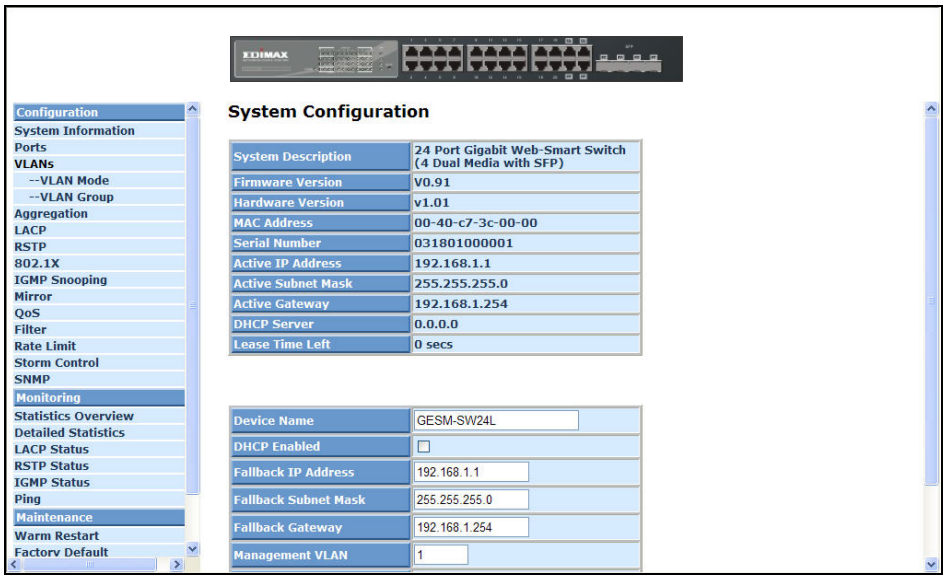


Fig. 2-9

First, IP Address: as shown in the Fig. 2-9, enter “192.168.1.1”. Assign an IP address of 192.168.1.x to you PC

Second, Subnet Mask: as shown in the Fig. 2-9, enter “255.255.255.0”. Any subnet mask such as 255.255.255.x is allowed in this case.

2-2. Typical Applications

The 24-Port GbE Web Smart Switch implements 24 Gigabit Ethernet TP ports with auto MDIX and four slots for removable modules Comprehensive fiber types of connection including LC and BiDi-LC SFP modules are supported. For more detailed specifications of the switch, please refer to Appendix A.

The switch is suitable for the following applications.

- Central Site/Remote Site is used in carrier or ISP applications. (See Fig. 2-10)
- Peer-to-peer is used for applications in between two remote offices. (See Fig. 2-11)
- Office network(See Fig. 2-12)

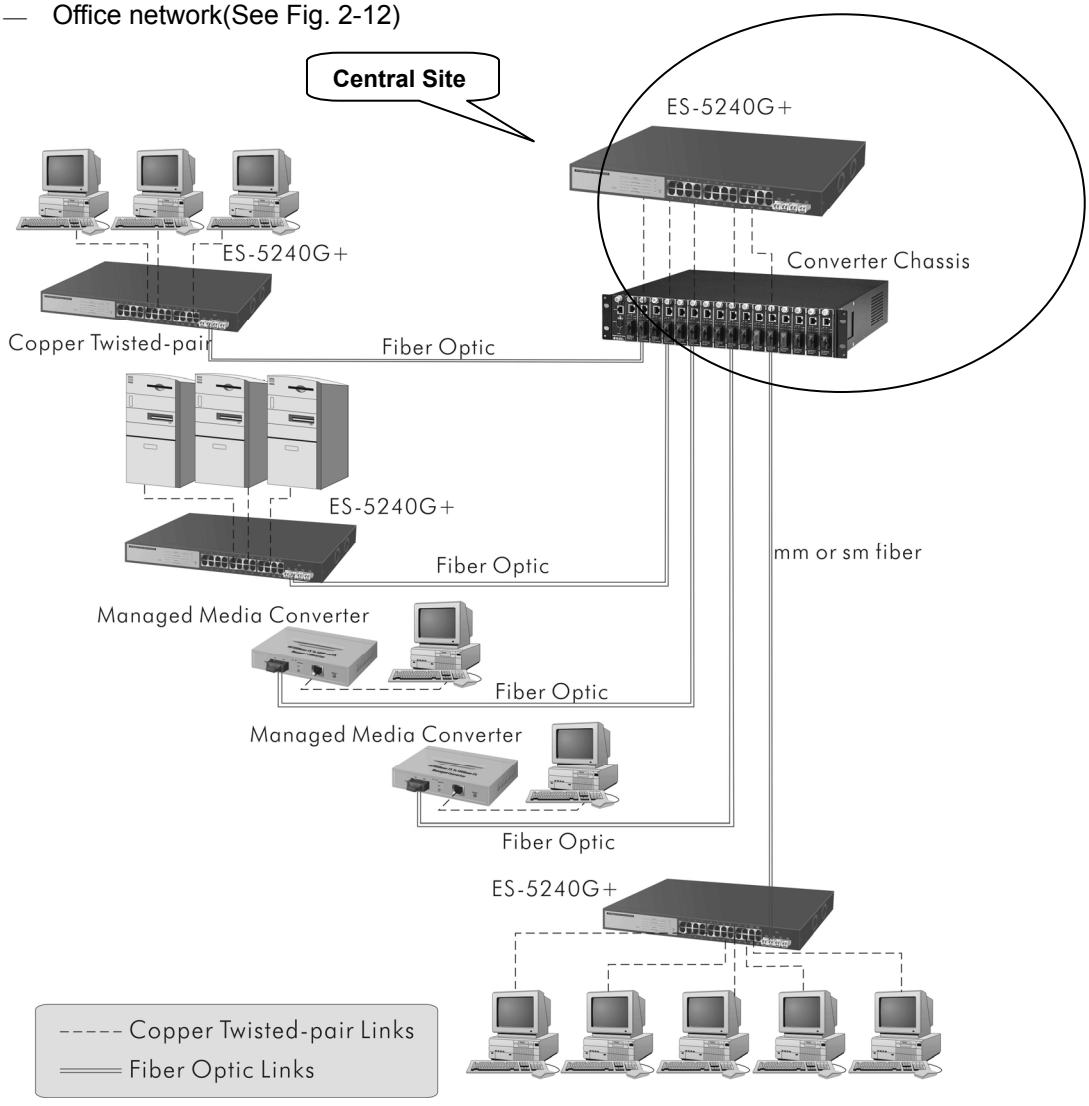


Fig. 2-10 Network Connection between Remote Site and Central Site

Fig. 2-10 is the reference diagram of a basic system wide connection scheme. This diagram demonstrates how this switch connects network devices and hosts.

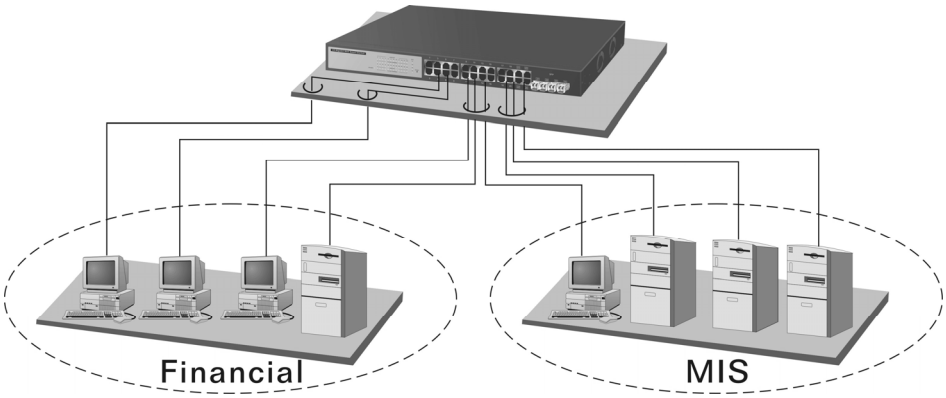


Fig. 2-11 Peer-to-peer Network Connection

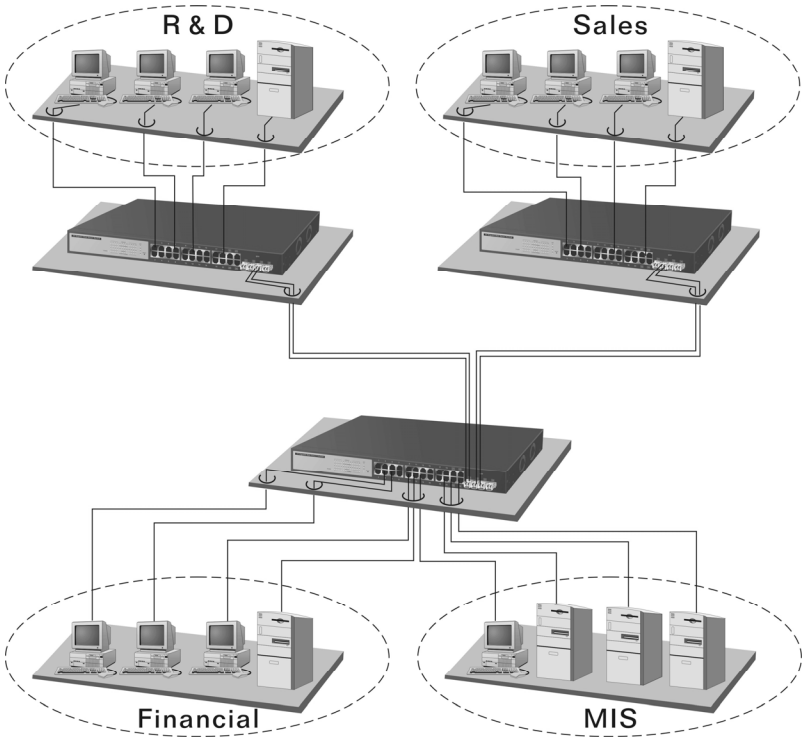


Fig. 2-12 Office Network Connection

3. Basic Concept and Management

In this chapter we are going to introduce you the basic concepts and features of Ethernet, and how to work with the management features provided by this switch.

3-1. What's the Ethernet

Ethernet originated and was implemented at Xerox in Palo Alto, CA in 1973 and was successfully commercialized by Digital Equipment Corporation (DEC), Intel and Xerox (DIX) in 1980. In 1992, Grand Junction Networks unveiled a new high speed Ethernet with the same characteristics of the original Ethernet but operated at 100Mbps, which is now called Fast Ethernet. This means Fast Ethernet inherits the same frame format, CSMA/CD and software interface. In 1998, Gigabit Ethernet rolled out and provided 1000Mbps. Now 10G/s Ethernet is under evaluation and may soon to be approved for practices. Although these Ethernet standards have different speed, same basic functions still apply. Same basic functions still apply. They are compatible in software and can connect each other almost without an issue. The transmission media may be the only limitation.

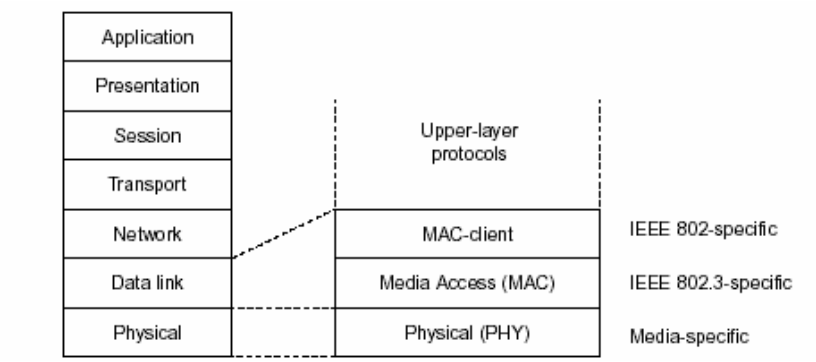
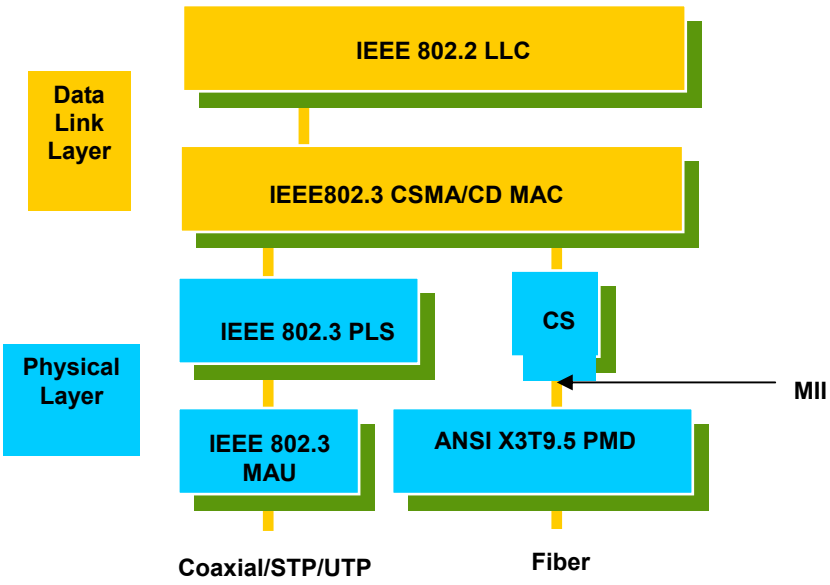


Fig. 3-1 IEEE 802.3 reference model vs. OSI reference mode

In Fig. 3-1, we can see that Ethernet locates at the Data Link layer and Physical layer and comprises three portions, including logical link control (LLC), media access control (MAC), and physical layer. The first two comprises Data link layer, which performs splitting data into frames for transmitting, receiving acknowledge frame, error checking and re-transmitting frames if not received correctly The Data link layer also provides an error-free channel upward to network layer.



The above diagram shows the Ethernet architecture in OSI model. LLC sub-layer and MAC sub-layer will respond to the Data Link layer, and the transceivers will respond to the Physical layer.

Logical Link Control (LLC)

Data link layer is composed of both the sub-layers of MAC and MAC-client. Here MAC client may be logical link control or bridge relay entity.

Logical link control acts as the interface between the Ethernet MAC and upper layers in the protocol stack, usually Network layer. Network layer has nothing to do with the nature of the LAN, so it operates over other different LAN technologies such as Token Ring, FDDI and so on. Likewise, as for the interface to the MAC layer, LLC defines the services provided by the interface independent medium access technology, which some natures of the medium itself apply.

DSAP address	SSAP address	Control	Information
8 bits	8 bits	8 or 16 bits	M*8 bits

DSAP address	=	Destination service access point address field
SSAP address	=	Source service access point address field
Control	=	Control field [16 bits for formats that include sequence numbering, and 8 bits for formats that do not (see 5.2)]
Information	=	Information field
*	=	Multiplication
M	=	An integer value equal to or greater than 0. (Upper bound of M is a function of the medium access control methodology used.)

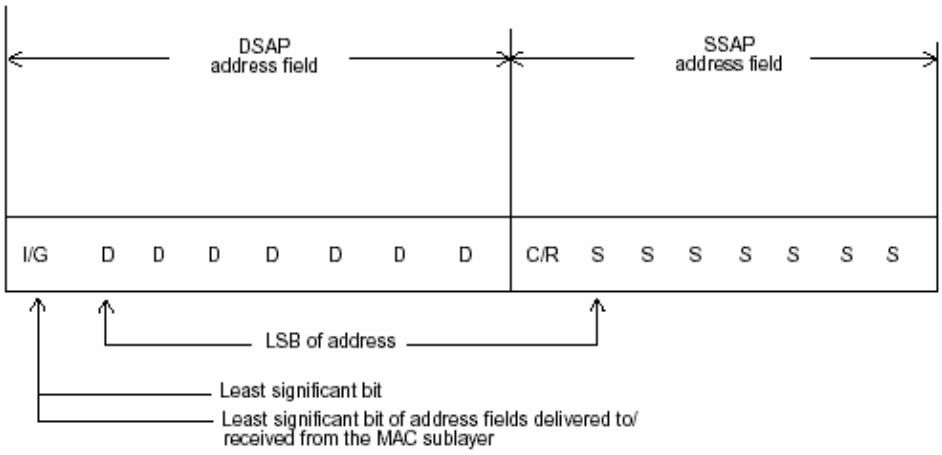
Table 3-1 LLC Format

The table 3-1 is the format of LLC PDU. It comprises four fields, DSAP, SSAP, Control and Information. The DSAP address field identifies the one or more service access points, in which the I/G bit indicates it is individual or group address. If all bits of DSAP are 1s, it's a global address. The SSAP address field identifies the specific services indicated by C/R bit (command or response). The DSAP and SSAP pair with certain reserved values indicates some well-known services listed in the table below.

0xAAAA	SNAP
0xE0E0	Novell IPX
0xF0F0	NetBios
0xFEFE	IOS network layer PDU
0xFFFF	Novell IPX 802.3 RAW packet
0x4242	STP BPDU
0x0606	IP
0x9898	ARP

Table 3-2

LLC type 1 connectionless service, LLC type 2 connection-oriented service and LLC type 3 acknowledge connectionless service are three types of LLC frame for all classes of service. In Fig 3-2, it shows the format of Service Access Point (SAP). Please refer to IEEE802.2 for more details.



I/G = 0 Individual DSAP
I/G = 1 Group DSAP
C/R = 0 Command
C/R = 1 Response

XODDDDDD DSAP address
XOSSSSSS SSAP address

X1DDDDDD Reserved for ISO definition
X1SSSSSS Reserved for ISO definition

Fig. 3-2 SAP Format

3-2. Media Access Control (MAC)

MAC Addressing

Because LAN is composed of many nodes, for the data exchanged among these nodes, each node must have its own unique address to identify who should send the data or should receive the data. In OSI model, each layer provides its own mean to identify the unique address in some form, for example, IP address in network layer.

The MAC belongs to Data Link Layer (Layer 2);the address is defined to be a 48-bit long and locally unique address. Since this type of addresses apply only to the Ethernet LAN media access control (MAC), they are referred to as MAC addresses.

The first three bytes are Organizational Unique Identifier (OUI) code assigned by IEEE. The last three bytes are the serial number assigned by the vendor of the network device. All these six bytes are stored in a non-volatile memory in the device. Their format is as the following table and normally written in the form of aa-bb-cc-dd-ee-ff, a 12 hexadecimal digits separated by hyphens, in which the aa-bb-cc is the OUI code and the dd-ee-ff is the serial number assigned by manufacturer.

Bit 47 bit 0

1st byte	2nd byte	3rd byte	4th byte	5th byte	6th byte
OUI code			Serial number		

Table 3-3 Ethernet MAC address

The first bit of the first byte in the Destination address (DA) determines the address to be a Unicast (0) or Multicast frame (1), known as I/G bit indicating individual (0) or group (1). So the 48-bit address space is divided into two portions, Unicast and Multicast. The second bit is for global-unique (0) or locally-unique address. The former is assigned by the device manufacturer, and the later is usually assigned by the administrator. In practice, global-unique addresses are always applied.

A unicast address is identified with a single network interface. With this nature of MAC address, a frame transmitted can exactly be received by the target's interface that the destination MAC points to.

A multicast address is identified with a group of network devices or network interfaces. In Ethernet, a many-to-many connectivity in the LANs is provided. It provides a mean to send a frame to many network devices at a time. When all bits of DA are 1s, it is a broadcast, which means all network devices except the sender itself can receive the frame and response.

Ethernet Frame Format

There are two major forms of Ethernet frame, type encapsulation and length encapsulation, both of which are categorized as four frame formats: 802.3/802.2 SNAP, 802.3/802.2, Ethernet II and Netware 802.3 RAW. We will introduce the basic Ethernet frame format defined by the IEEE 802.3 standard required for all MAC implementations. A basic Ethernet frame format contains seven fields as explained below:

PRE	SFD	DA	SA	Type/Length	Data	Pad bit if any	FCS
7	7	6	6	2	46-1500		4

Fig. 3-3 Ethernet frame structure

- **Preamble (PRE)** —The PRE is 7-byte long with alternating pattern of ones and zeros used to tell the receiving node that a frame is coming, and to synchronize the physical receiver with the incoming bit stream. The preamble pattern is:

  10101010 10101010 10101010 10101010 10101010 10101010 10101010

- **Start-of-frame delimiter (SFD)** — The SFD is one-byte long with alternating pattern of ones and zeros, ending with two consecutive ones. It immediately follows the preamble and uses the last two consecutive 1s bit to indicate that the next bit is the start of the data packet and is the left-most bit of the left-most byte of the destination address. The SFD pattern is 10101011.
-

- **Destination address (DA)** — The DA field is used to identify which network device(s) should receive the packet. It is a unique address. Please see the section of MAC addressing.

- **Source addresses (SA)** — The SA field indicates the source node. The SA is always an individual address and the left-most bit in the SA field is always 0.

- **Length/Type** — This field indicates either the number of the data bytes contained in the data field of the frame, or the Ethernet type of data. If the value of first two bytes is less than or equal to 1500 in decimal, the number of bytes in the data field is equal to the Length/Type value, i.e. this field acts as Length indicator at this moment. When this field acts as Length, the frame has optional fields for 802.3/802.2 SNAP encapsulation, 802.3/802.2 encapsulation and Netware 802.3 RAW encapsulation. Each of them has different fields following the Length field.
- If the Length/Type value is greater than 1500, it means the Length/Type acts as Type. Different type value means the frames of different protocols running over Ethernet being sent or received.

For example,

0x0800	IP datagram
0x0806	ARP
0x0835	RARP
0x8137	IPX datagram
0x86DD	IPv6

- **Data** — Less than or equal to 1500 bytes and greater or equal to 46 bytes. If data is less than 46 bytes, the MAC will automatically extend its length by padding bits and have the payload be equal to 46 bytes. The length of data field must equal the value of the Length field when the Length/Type acts as Length.

- **Frame check sequence (FCS)** — This field contains a 32-bit cyclic redundancy check (CRC) value, and is a check sum computed with DA, SA, through the end of the data field with the following polynomial.

$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

- It is created by the sending MAC, and then recalculated by the receiving MAC to check it the packet is valid or not.

How does a MAC work?

The MAC sub-layer has two primary jobs to do:

1. *Receiving and transmitting data*. When receiving data, it parses frame to detect error; when transmitting data, it performs frame assembly.
2. *Performing Media access control.* It prepares the initiation jobs for a frame transmission and makes recovery from transmission failure.

Frame transmission

As Ethernet adopted Carrier Sense Multiple Access with Collision Detect (CSMA/CD), it detects if there is any carrier signal from another network device running over the physical medium when a frame is ready for transmission. This is referred to as sensing carrier, also “Listen”. If there is signal on the medium, the MAC defers the traffic to avoid a transmission collision and waits for a random period of time, called backoff time, then sends the traffic again.

After the frame is assembled, when transmitting the frame, the preamble (PRE) bytes are inserted and sent first. Next sart of frame Delimiter (SFD), DA, SA and through the data field and FCS field in turn. The followings summarize what a MAC does before transmitting a frame.

1. MAC will assemble the frame. First, the preamble and Start-of-Frame delimiter will be put in the fields of PRE and SFD, followed by DA, SA, tag ID (if tagged VLAN is applied). Ethertype or the value of the data length, and payload data field Finally, assemble the FCS data in order and put it into the responded fields.
2. Listen if there is any traffic running over the medium. If yes, wait.
3. If the medium is quiet, and no longer senses any carrier, the MAC waits for a period of time, i.e. inter-frame gap time to have the MAC ready with enough time and then start transmitting the frame.
4. During the transmission, MAC keeps monitoring the status of the medium. If no collision happens till the end of the frame, it transmits successfully. If there has been a collision, the MAC will send the patterned jamming bit to guarantee the collision event propagated to all involved network devices, then wait for a random period of time, i.e. backoff time. When backoff time expires, the MAC goes back to the beginning state and attempts to transmit again. After a collision happens, MAC increases the transmission attempts. If the count of the transmission attempt reaches 16 times, the frame in MAC’s queue will be discarded.

Ethernet MAC transmits frames in half-duplex and full-duplex ways. In half-duplex operation mode, the MAC can either transmit or receive frame at a moment, but cannot do both jobs at the same time.

As the transmission of a MAC frame with half-duplex operation exists only in the same collision domain. The carrier signal needs to spend time to travel and reach the target device. The worst case occurs when two most-distanced devices in the same collision domain; one sends the frame first and the other sends the frame right before the frame from first device arrives. The collision happens and will be detected by the second device immediately. Because of the medium delay, this corrupted signal needs to spend some time to propagate back to the first device. The maximum time to detect a collision is approximately twice the signal propagation time between the two most-distant devices. This maximum time is traded-off by the collision recovery time and the diameter of the LAN.

In the original 802.3 specification, Ethernet operates in half duplex only. Under this condition, when in 10Mbps LAN, it's 2500 meters, in 100Mbps LAN, it's approximately 200 meters and in 1000Mbps, 200 meters. Theoretically, the LAN diameter should be 20 meters. However, in practice the LAN diameter of 200 meters is kept by increasing the minimum frame size with a variable-length, non-data extension bit field, which is removed by the receiving MAC. The following tables are the frame format suitable for 10M, 100M and 1000M Ethernet, and some parameters that shall be applied to all of these three types of Ethernet.

Actually, the Gigabit Ethernet chips in practice do not support this feature at the moment. All chips, and as well as all network vendors' devices, support full-duplex mode only. It is safe to say that this criterion does not exist for both present time and in the future. The switch's Gigabit module supports only full-duplex mode.

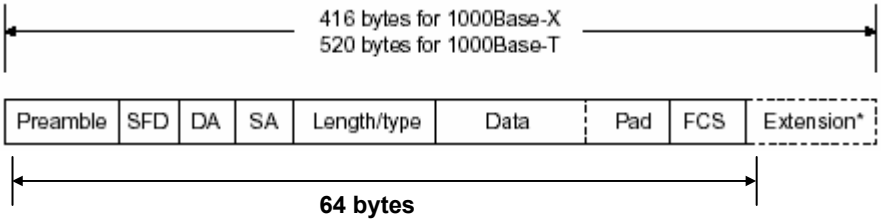
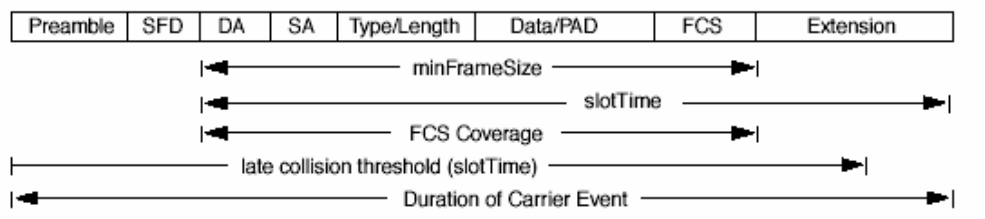


Fig. 3-4 Gigabit Ethernet Frame

Parameter value/LAN	10Base	100Base	1000Base
Max. collision domain DTE to DTE	100 meters	100 meters for UTP 412 meters for fiber	100 meters for UTP 316 meters for fiber
Max. collision domain with repeater	2500 meters	205 meters	200 meters
Slot time	512 bit times	512 bit times	512 bit times
Interframe Gap	9.6us	0.96us	0.096us
AttemptLimit	16	16	16
BackoffLimit	10	10	10
JamSize	32 bits	32 bits	32 bits
MaxFrameSize	1518	1518	1518
MinFrameSize	64	64	64
BurstLimit	Not applicable	Not applicable	65536 bits

Table 3-4 Ethernet parameters for half duplex mode



In full-duplex operation mode, both transmitting and receiving frames are processed simultaneously. This doubles total effective bandwidth. Full duplex is much easier than half duplex because it does not involve media contention, collision, retransmission schedule and padding bits for short frame. The rest functions follow the specification of IEEE802.3. For example, it must meet the requirement of minimum inter-frame gap between successive frames and frame format remains the same as that in the half-duplex operation.

Because no collision will occur in full-duplex operation, there is no mechanism to tell all the involved devices. What will it be if the receiving device is busy and a frame is coming at the same time? Can it use “backpressure” to tell the source device? A function flow control is this introduced in the full-duplex operation.

3-3. Flow Control

Flow control is a mechanism to tell the source device stop sending frames for a specified period of time designated by target device until the PAUSE time expires. This is accomplished by sending a PAUSE frame from target device to source device. When the target is not busy and the PAUSE time is expired, it will send another PAUSE frame with zero time-to-wait to source device. After the source device receives the PAUSE frame, it will again transmit frames immediately. PAUSE frame is identical in the form of the MAC frame with a pause-time value and with a special destination MAC address 01-80-C2-00-00-01. As per the specification, PAUSE operation can not be used to inhibit the transmission of MAC control frame.

Normally, in 10Mbps and 100Mbps Ethernet, only symmetric flow control is supported. However, some switches (e.g. 24-Port GbE Web Smart Switch) support not only symmetric but also asymmetric flow controls for special applications. In Gigabit Ethernet, both symmetric flow control and asymmetric flow control are supported. Asymmetric flow control only allows transmitting PAUSE frame in direction way from one side, the other side does not but only receive and discard the flow control information. Symmetric flow control allows both two ports to transmit PASUE frames to each other simultaneously.

Inter-frame Gap time

After the end of a transmission, if a network node is ready to transmit data out and if there is no carrier signal on the medium at that time, the device will wait for a period of time known as an inter-frame gap time to have the medium clear and stabilized as well as to have the jobs ready, such as adjusting buffer counter, updating counter and so on, at the receiver site. Once the inter-frame gap time expires after the de-assertion of carrier sense, the MAC transmits data. In IEEE802.3 specification, this is 96-bit time or more.

Collision

Collision happens only in half-duplex operation. When two or more network nodes transmit frames at approximately the same time, a collision will always occur and interfere with each other. This results the carrier signal distorted and un-discriminated. When a collision is detected during a frame transmission, the transmission will not stop immediately but, instead, continue transmitting until the rest bits specified by jamSize are completely transmitted. This guarantees the duration of collision to be enough to have all involved devices able to detect the collision. This is referred to as Jamming. After jamming pattern is sent, MAC stops transmitting the rest data queued in the buffer and waits for a random period of time, known as backoff time with the following formula. When backoff time expires, the device goes back to the state of attempting to transmit frames. The backoff time is determined by the formula below. When the times of collision is increased, the backoff time is getting longer until the collision times excess 16. If this happens, the frame will be discarded and backoff time will also be reset.

$$0 \le r < 2^k$$

where

k = min (n, 10)

Frame Reception

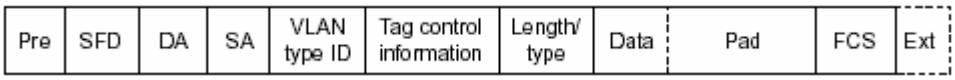
In essence, the frame reception is the same in both operations of half duplex and full duplex, except that full-duplex operation uses two buffers to transmit and receive the frame independently. The receiving node always “listens” if there is traffic running over the medium when it is not receiving a frame. When a frame destined for the target device comes, the receiver of the target device begins receiving the bit stream, and looks for the PRE (Preamble) pattern and Start-of-Frame Delimiter (SFD) that indicates the next bit is the starting point of the MAC frame until all bit of the frame is received.

For a received frame, the MAC will check:

1. If it is less than one slotTime in length, i.e. short packet, and if yes, it will be discarded by MAC because, by definition, the valid frame must be longer than the slotTime. If the length of the frame is less than one slotTime, there may be a collision happened somewhere or an interface malfunctioned in the LAN. When detecting the case, the MAC drops the packet and goes back to the ready state.
2. The DA of received frame should match the physical address of the receiving MAC or the address of the to be recognized designated multicast. If not, the frame will be discarded and the MAC will pass the frame to its client and go back to ready state.
3. If the frame is too long; if yes, the frame will be thrown away and a Too Long frame will be reported.
4. please note that this kind of sentence is fragment and not grammatically correct. If not, for 10M and 100M Ethernet, discards the frame. For Gigabit Ethernet or higher speed Ethernet, MAC has to check one more field, i.e. extra bit field, to see if FCS is invalid. to see if FCS is invalid.To meet the specification of IEEE 802.3, the MAC will check to see if there any extra bits exist. When both FCS and extra bits are valid, the received frame will be accepted; otherwise the received frame will be discarded and a frameCheckError will be reported if no extra bit appended, or an alignmentError will be reported if extra bits appended.
5. If the length/type is valid; if not, the packet will be discarded and a lengthError will be reported.
6. If all above five procedures are processed without any error, the MAC will treat the frame as a good one and start to disassemble the frame.

What if a VLAN tagging is applied?

VLAN tagging is a 4-byte long data immediately following the MAC source address. When tagged VLAN is applied, the Ethernet frame structure will have a little change shown as follows.



Only two fields, VLAN ID and Tag control information are different in comparison with the basic Ethernet frame. The rest fields are the same.

The first two bytes is VLAN type ID with the value of 0x8100 indicating the received frame is tagged VLAN and the next two bytes are Tag Control Information (TCI) used to provide user priority and Both VLAN ID and TCI will be explained in the following table.

Bits 15-13	User Priority 7-0, 0 is lowest priority
Bit 12	CFI (Canonical Format Indicator) 1: RIF field is present in the tag header 0: No RIF field is present
Bits 11-0	VID (VLAN Identifier) 0x000: Null VID. No VID is present and only user priority is present. 0x001: Default VID 0xFFF: Reserved

Table 3-5

Note: RIF is used in Token Ring network to provide source routing and comprises two fields, Routing Control and Route Descriptor.

When MAC parses the received frame and finds a reserved special value 0x8100 at the location of the Length/Type field of the normal non-VLAN frame, it will interpret the received frame as a tagged VLAN frame. If this happens in a switch, the MAC will forward it, according to its priority and egress rule, to all the ports that is associated with that VID. If it happens in a network interface card, MAC will deprive off the tag header and process it in the same way as a basic normal frame. For a VLAN-enabled LAN, all involved devices must be equipped with VLAN optional function.

At operating speeds above 100 Mbps, the slotTime employed at slower speeds is inadequate to accommodate network topologies of the desired physical extent. Carrier Extension provides a means by which the slotTime can be increased to a sufficient value for the desired topologies, without increasing the minFrameSize parameter, as this would have deleterious effects. Nondata bits, referred to as extension bits, are appended to frames that are less than slotTime bits in length so that the resulting transmission is at least one slotTime in duration. Carrier Extension can be performed only if the underlying physical layer is capable of sending and receiving symbols that are readily distinguished from data symbols, as is the case in most physical layers that use a block encoding/decoding scheme.

The maximum length of the extension is equal to the quantity (slotTime - minFrameSize). The MAC continues to monitor the medium for collisions while it is transmitting extension bits, and it will treat any collision that occurs after the threshold (slotTime) as a late collision.

3-4. How does a switch work?

The switch is a layer 2 Ethernet Switch equipped with 24 Fast Ethernet ports and 2 optional modules which support Gigabit Ethernet or 100M Ethernet. Each port on it is an independent LAN segment and thus has 26 LAN segments and 26 collision domains, contrast to the traditional shared Ethernet HUB in which all ports share the same media and use the same collision domain and thus limit the bandwidth utilization. With switch's separated collision domain, it can extend the LAN diameter farther than the shared HUB does and highly improve the efficiency of the traffic transmission.

Due to the architecture, the switch can provide full-duplex operation to double the bandwidth per port and many other features, such as VLAN, bandwidth aggregation and so on, that are not supported in a shared hub.

Terminology

Separate Access Domains:

As per the description in the section of "What's the Ethernet", Ethernet utilizes CSMA/CD to arbitrate who can transmit data to the station(s) attached in the LAN. When more than one station transmits data within the same slot time, the signals will collide, referred to as collision. The arbitrator will arbitrate who should gain the media. The arbitrator is a distributed mechanism in which all stations contend to gain the media. Please refer to "What's the Ethernet" for more details.

In Fig.3-5, assumed in half duplex, you will see some ports of the switch are linked to a shared HUB, which connects many hosts, and some ports are individually linked to a single host. The hosts attached to a shared hub will be in the same collision domain, separated by the switch, and use CSMA/CD rule. For the host directly attached to the switch, because no other host(s) joins the traffic contention, hence it will not be affected by CSMA/CD. These LAN segments are separated in different access domains by the switch.

Micro-segmentation:

To have a port of the switch connected to a single host is referred to as micro-segmentation. It has the following interesting characteristics.

- Access contention (e.g. Collision) is not necessary. Each micro-segment has its own access domain; however, collision can still occur between each host and the switch port.
- When performing the full duplex, the collision vanishes.
- The host owns a dedicated bandwidth of the port.

The switch port can run at different speed, such as 10Mbps, 100Mbps or 1000Mbps. A shared hub cannot.

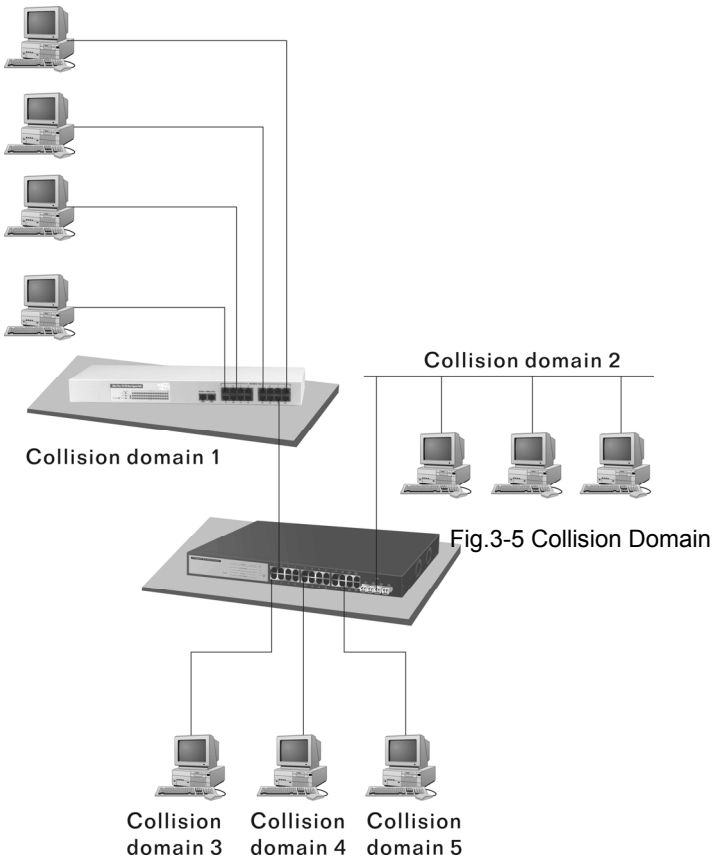


Fig.3-5 Collision Domain

Extended Distance Limitations:

The diameter of a half-duplex LAN segment is determined by its maximum propagation delay time. For example, in 10M LAN, the most distance of a LAN segment using cable is 2500 meters and 185 meters when using coaxial cable. The switch with its per port per collision domain can extend the distance like a bridge does. And what's more, when operating in full-duplex mode, the distance can reach farther than half duplex because it is not limited by the maximum propagation delay time (512 bits time). If fiber media is applied, the distance can be up to tens of kilometers.

Traffic Aggregation:

Traffic aggregation is to aggregate the bandwidth of more than one port and treat it as a single port ina LAN. This single port possesses all the features of a normal port but loading balance. This is a great feature for a port which needs more bandwidth when cost more for higher bandwidth is not possible.

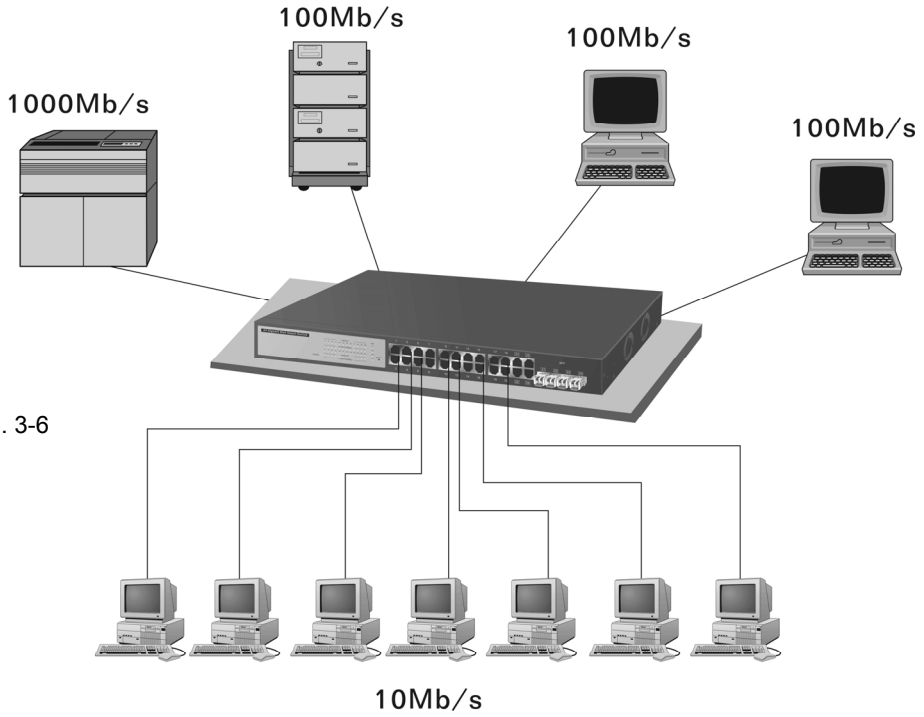


Fig. 3-6

How does a switch operate?

A Layer 2 switch uses some features of the Data Link layer in OSI model to forward the packet to destination port(s). Here we introduce some important features of a switch and how they work.

MAC address table

When a packet is received on a port, the switch first checks if the packet is good or bad and extracts the source MAC address (SA) and destination MAC address (DA) to find 1) if SA exists in the MAC address table, if it does not, the switch will put it in the MAC address table; if it does, 2) the switch looks up DA and its associated port to which the traffic is forwarded. If DA does not exist, the switch will broadcast the packet.

Due to the limitation to the size of a MAC address, the MAC address aging function is applied. When the MAC address has resided and no updates been refreshed in the table for a long time, this means the traffic using that entry has not come for a while. If this time period is more than the aging time, the entry will be marked invalid. The vacancy is now available for other new MAC.

Both learning and forwarding are the most important functions in a switch. Besides that, VLAN can be one of the rules to forward packets. There are ingress rule and egress rule applied. The ingress rule is used to filter the incoming packet by VLAN ID and so on and to decide whether the packet is allowed to enter the switch or not. The egress rule is used to forward the packet to the proper port.

Mac address aging

There is a field in MAC address table used to put the entry's Age time which determines how long a MAC entry can reside in a switch. The age time is refreshed when a packet with that SA arrives. Usually, the age time is programmable.

Transmission schedule

In most layer 2 switches, the QoS is supported. QoS in a switch must associate a transmission schedule to transmit the packet. This function is much to do with the priority level that a packet has. With a given priority, the scheduler will do the proper action on it. The scheduler has many ways to implement, and different chips may support different schedule algorithms. Most common schedulers are:

FCFS: First Come First Service.

Strictly Priority: All High before Low.

Weighted Round Robin:

Set a weight figure to the packet with a priority level, say 5-7, and next, set another weight to the packet with a priority level, say 2-4 and so on. The WRR will transmit the packet with the weight. So the packet of each priority level can be allocated within a fixed bandwidth.

Bandwidth rating

Bandwidth rating is the limitation set by administrator, and it can be applied to those with SLA. Bandwidth rating can be total bandwidth, types of service of a port with many steps. The switch supports by-port Ingress and Egress total bandwidth rate control capacity. The bandwidth rate resolution is 0.1 Mbps (100Kbps) and ranges from 0 to 100Mbps.

3-5. Virtual LAN

What is a VLAN?

It is a subset of a LAN. Before we discuss VLAN, we must understand what LAN is. In general, a LAN is composed of different physical network segments bridged by switches or bridges which attach to end stations in the same broadcast domain. The traffic can reach any station on the same LAN. Beyond this domain, the traffic cannot go without router's help. This also implies that a LAN is limited. If you need to communicate with the station outside the LAN, a router is needed which always lies on the edge of the LAN.

For a layer 2 VLAN, it assumes it is a logical subset of a physical LAN separated by specific rules such as tag, port, MAC address and so on. In other words, they can communicate with each other between separated small physical LANs within a LAN but can not in between any two separated logical LANs.

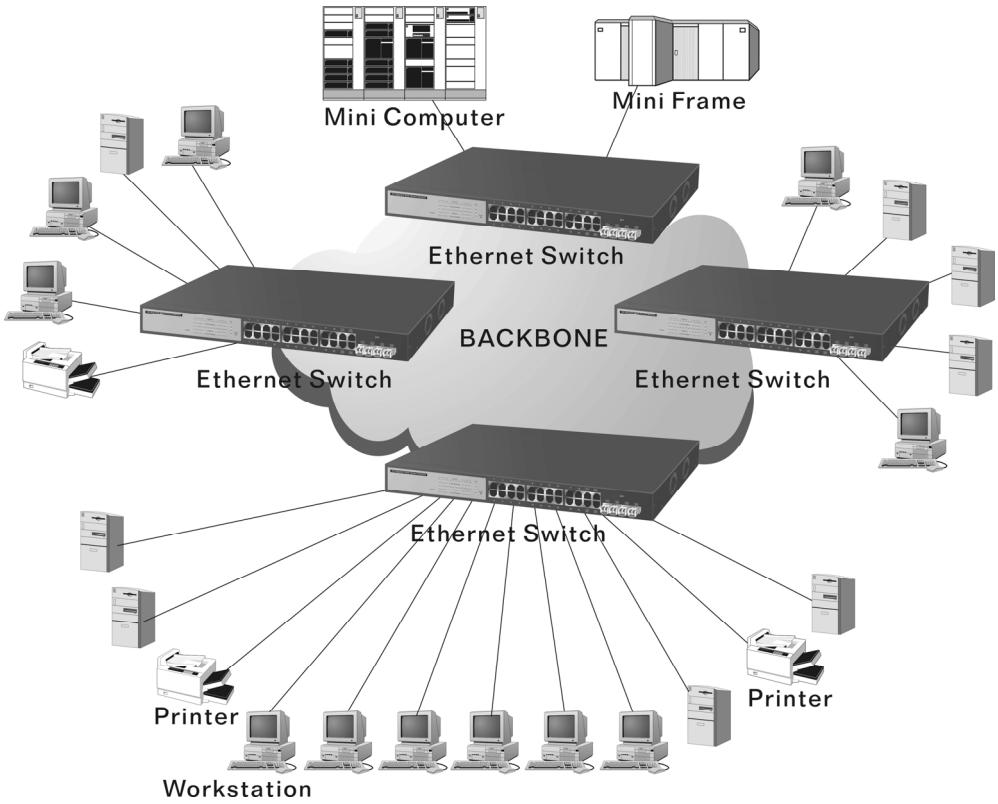


Fig. 3-7

In the figure above, all stations are within the same broadcast domain. For these stations, it is obviously that the traffic is getting congested while adding more stations on it. With the more and more users joining the LAN, broadcast traffic will rapidly decrease the performance of the network. The network may eventually go down.

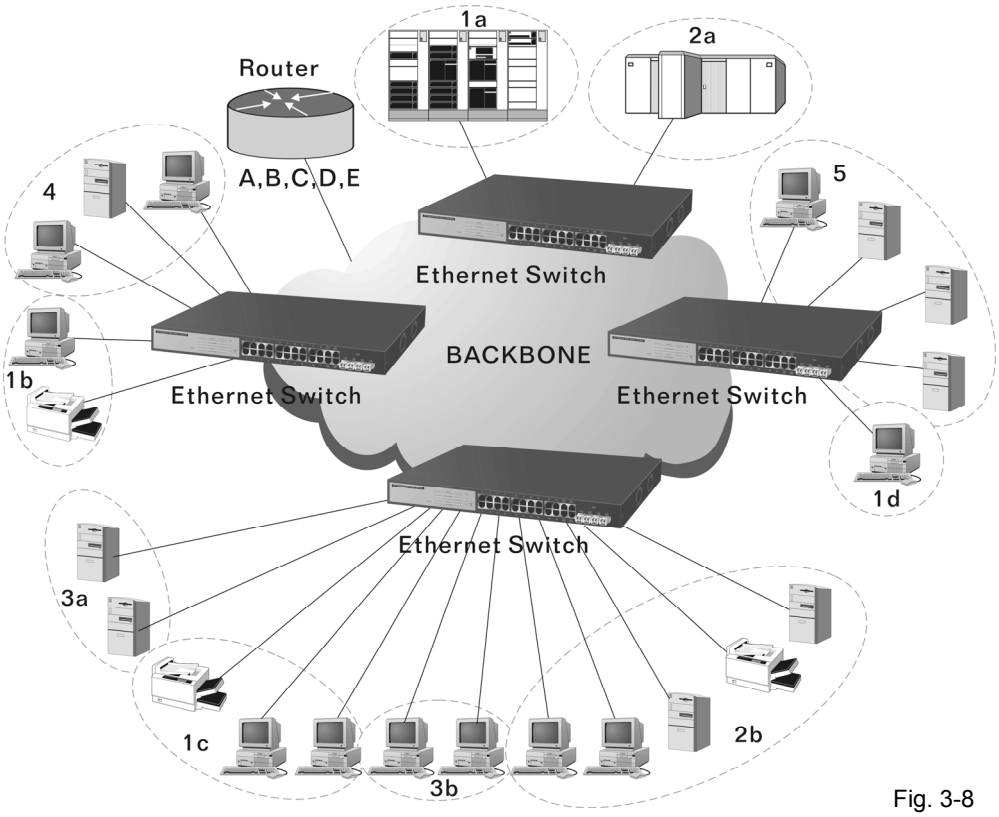


Fig. 3-8

Now we apply VLAN technology to configure the system shown as the figure above. We can partition the users into the different logical networks which have their own broadcast domain. The traffic will not disturb among these logical networks. The users 1x (x denotes a ~ d) are members of VLAN 1. Any traffic within VLAN 1 does not flow to VLAN 2 and others. This helps us configure the network easily according to the criteria needed, for example, financial, accounting, R&D and whatever you think it necessary. You can also easily move a user to a different location or join a new user somewhere in the building to VLAN. It will not be as easy without VLAN. Basically, VLAN can easily provide the following 3 benefits: move and change users, reduce broadcast traffic and increase performance, Security.

Besides, VLAN can highly reduce the traffic congestion and increase total performance because there are not as many users in the same broadcast domain.

There are many types of VLAN applied. The most popular ones are port-based VLAN, tag-based VLAN and protocol-based VLAN.

- Port-based VLAN

  Some physical ports are configured as members of a VLAN. All stations attached on these ports can communicate with each other.

- Tag-based VLAN

  It identifies the membership by VLAN ID, no matter where the packet comes from. It is also referred to as 802.1Q VLAN.

- Protocol-based VLAN

  It identifies the VLAN membership by layer 3 protocol types, for example IPX, Appletalk, IP, etc.

Other VLAN technologies not mentioned above are MAC-based VLAN, IP-based VLAN and so on.

Terminology

Tagged Frame:

A frame, carrying a tag field following the source MAC address, is four bytes long and contains VLAN protocol ID and tag control information composed of user priority, Canonical Format Indicator (CFI) and optional VLAN identifier (VID). Normally, the maximal length of a tagged frame is 1522 bytes.

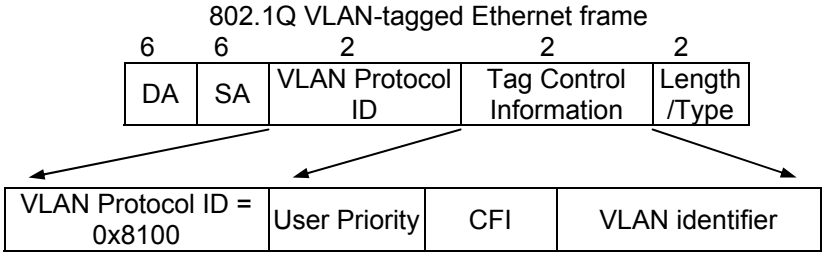


Fig.3-9 Tag Format

VLAN Protocol ID: 8100 is reserved for VLAN-tagged frame.

User Priority: 3 bits long. User priority is defined to 7 – 0. 0 is the lowest priority.

CFI: Canonical Format Indicator. 1 bit long. It is used to encapsulate a token ring packet to let it travel across the Ethernet. Usually, it is set to 0.

VLAN ID: 12 bits long. 0 means no VLAN ID is present. 1 means default VLAN, 4095 reserved.

VLAN-tagged frame:

An Ethernet frame, carrying VLAN tag field, contains VLAN identification without the value of 0 and 4095, and priority information.

Priority-tagged frame:

An Ethernet frame, carrying VLAN tag field, contains VLAN identification with the value of 0 and priority information.

Untagged frame:

An Ethernet frame carries no VLAN tag information.

VLAN Identifier:

Also referred to as VID. It is used to identify a member whether it belongs to the VLAN group with the VID. The assignable number is 1- 4094. If VID=0, the tagged frame is a priority packet. Both the value of 0 and 4095 also cannot be assigned in VLAN management.

Port VLAN Identifier:

VLAN identifier of a port. It is also referened to as PVID. When an untagged frame or a priority-tagged frame is received, the PVID of that port will be inserted in the VLAN tag field of the frame. This frame with VID assigned by a port is called PVID. Each port can only be assigned one PVID. The default value for PVID is 1, which is the same as VID.

Ingress filtering:

This is the process to check a received packet and compare its VID to the VLAN membership of the ingress port. The ingress filtering can be set by per port. When receiving a packet, the VLAN bridge will examine if the VID in the frame's header presents.

If the VID of the received packet presents, the VID of the packet is used. The VLAN bridge will check its MAC address table to see if the destination ports are members of the same VLAN. If both are members of the tagged VLAN, then the packet will be forwarded.

If the packet is untagged or a null tag packet, the ingress port's PVID is applied to the packet. The VLAN bridge will then look up the MAC address table and determine as which ports the packet should be forwarded to. Next, it will check to see if the destination ports belong to the same VLAN with that PVID. If the destination ports are members of the VLAN used by ingress port, the packet will be forwarded.

Note: VID can not be 0 or 4095.

Ingress Rule:

Each packet received by a VLAN-aware bridge will be classified to a VLAN. The classification rule is described as follows.

1. If the VID of the packet is null (VID=0) or this packet is an untagged packet:
   a. If there are still some other ways(e.g. protocol, MAC address, application, IP-subnet, etc.) to classify the incoming packets beside port-based classification in implement and these approaches can offer non-zero VID, then, use the value of VID offered by other classifications for VLAN's classification.
   b. If there is only port-based classification in implement or other classification approaches cannot offer non-zero VID for the incoming packets, then assign the PVID to the incoming packets as VID for the classification of the VLAN group.
2. If the VID is not a null (VID≠0), then use the value to classify the VLAN group.

Egress Rule:

An egress list is used to make the tagging and forwarding decision on an outgoing port. It specifies the VLANs whose packets can be transmitted out and specifies if the packet should be tagged or not. It can be configured for port's VLAN membership, and tagged or untagged for a transmitted packet. When a packet is transmitted out, the VLAN bridge checks the port's egress list. If the VLAN of the packet is on the egress list of the port which the packet is designated to, the packet will be transmitted with the priority accordingly. If enabled, an egress port will transmit out a tagged packet if the port is connected to a 802.1Q-compliant device. If an egress port is connected to a non-802.1Q device or an end station, the VLAN bridge must transmit out an untagged packet, i.e. the tag has been stripped off in an egress port. Egress rule can be set by per port.

Independent VLAN Learning (IVL):

It specifies the mode how to learn MAC address. For a specified VLAN, it will use an independent filtering database (FID) to learn or look up the membership information of the VLAN and decide where to go.

Shared VLAN Learning (SVL):

In this mode, some VLAN or all VLANs use the same filtering database storing the membership information of the VLAN to learn or look up the membership information of the VLAN. In 24-Port GbE Web Smart Switch, you can choose a VID for sharing filtering database in Shared VID field if you wish to use the existed filtering database. For a specified VLAN, when a MAC address is learned by a switch, VLAN will use this formation to make forwarding decision.

Filtering Database:

Referred to as FID. It can provide the information where the packet will be sent to. Filtering database will supply the outgoing port according to the request from forwarding process with VID and DA. When a packet is received, if it has a non-zero VID, then FID will offer the associated outgoing ports information to the packet.

In SVL, VLANs use the same Filtering Database. In IVL, VLANs use different FIDs. Any VID can be assigned to the same FID by administrator

How does a Tagged VLAN work?

If the ingress filtering is enabled and when a packet is received, the VLAN bridge will first check if the VID of the packet presents.

1). If the packet has a non-zero VID, the VLAN bridge will apply this VID as the VLAN
ID of the packet in the network.

2). For a packet with a null tag or no VLAN tag, if the VLAN bridge provides rules to decide its VID, then this VID is applied to the packet.

If the VLAN bridge does not support any rule for VID, then apply the PVID of the port to the packet which came from that port. The VLAN bridge checks to see if the ingress port and the received packet are on the same VLAN. If not, drop the packet. If yes, forwards it to the associated ports. Meanwhile, this VLAN must be applied to the egress port, or the packet will be dropped.

If ingress filtering is disabled, the VLAN bridge will only check the MAC address table to see if the destination VLAN exists. If VLAN does not exist, then drop the packet; and if both DA and VLAN do not exist, forward the packet. If VLAN is only known to exist, then floods the packet to all the ports the VLAN covers.

If we plan to deploy four VLANs in an office and use a switch to partition them, we need to check the ports/VLAN assignment first. Assuming a 24-port switch is applied.

Name	VID	Port Members
Marketing	2	1,2,3,4,5
Service	3	6,7,20,21,22
Sales	4	8,9,10,11,12,13,14,15,16
Administration	1	17,18,19,23,24

Table 3-6

Next, assign IP address to each VLAN. Practically, we use 10.x.x.x as local IP block. Because there are total four VLANs in the network, we must assign 4 IP blocks to each of them.

Name	VID	Network Address
Marketing	2	10.1.2.0/24
Service	3	10.1.3.0/24
Sales	4	10.1.4.0/24
Administration	1	10.1.1.0/24

Table 3-7

Here we apply the subnet mask 255.255.255, and each VLAN is capable of supporting 254 nodes.

3-6. Link Aggregation

Basically, Link Aggregation is to aggregate the bandwidth of more than one port to an assigned logical link. This highly increases total bandwidth to the targeted device. There is more than one Link Aggregation technology in many vendors' switch products already, which may cause the problem of interoperability. This is the reason why now we have 802.3ad Link Aggregation Control Protocol (LACP).

Why 802.3ad (LACP)?

Network is varying. For example, if a port malfunctioned or unplugged accidentally in a static trunk port, administrator has to reconfigure it, or the network will get in trouble. Therefore, offering a tool with automatic recovery capability is necessary for an administrator. LACP is a protocol that allows a switch to be able to know whether its partner has the capability to co-setup a trunk between them.

Usually, if administrator wishes to increase the bandwidth of a specific link, he may:

1. Buy new network equipments with higher throughput, or
2. Aggregate the bandwidth of more than one port to become a local link.

If item 1 is the case, you will have to pay much more for the equipments; and the results may not be scalable if the unsatisfied performance is caused by hardware limitations.

If item 2 is the case, no extra cost is required, and the demand of bandwidth can be flexible because all that needs is to reconfigure equipments that are there already. And what's more, no worries necessary regarding the interoperability issue. Applying LACP in your network, you will not only gain benefits as listed below to improve the performance of your network but also have these investments reusable to future new network bandwidth planning.

Public standardized specification

1. No interoperability issue
2. No change to IEEE 802.3 frame format, no change necessary for software and management.
3. Increased bandwidth and availability
4. Load sharing and redundancy
5. Automatic configuration
6. Rapid configuration and reconfiguration
7. Determinated behavior
8. Low risk of duplication or mis-ordering
9. Support existing IEEE 802.3 MAC Clients
10. Backward compatibility with aggregation-unaware devices

There are also some constraints when applying LACP.

1. LACP does not support inter-switch bandwidth aggregation.
2. The ports aggregated must operate in full-duplex mode.
3. The ports in the same Link Aggregation Group must have the same speed, for example, all with 100Mbps or all 1000Mbps. You cannot aggregate a 1000Mbps and two 100Mbps for a 1.2Gbps trunk port.

Terminology

Link Aggregation:

It is a method to have multiple physical links with the same media and speed bundled to be a logical link forming a Link Aggregation Group with a group ID. With the viewpoint of MAC client, each Link Aggregation Group is an independent link.

There are three cases of link used in the network, which are switch to switch, switch to station and station to station. Here a station may be a host or a router.

Link Aggregation, called port trunking sometimes, has two types of link configuration, including static port trunk and dynamic port trunk.

- Static Port Trunk:

  When physical links are changed, administrator needs to manually configure the switches one by one.

- Dynamic Port Trunk:

  When physical links are changed, LACP takes over and automatically reconfigure. Administrator does not have to do anything and may see the trap message of LACP changed in NMS.

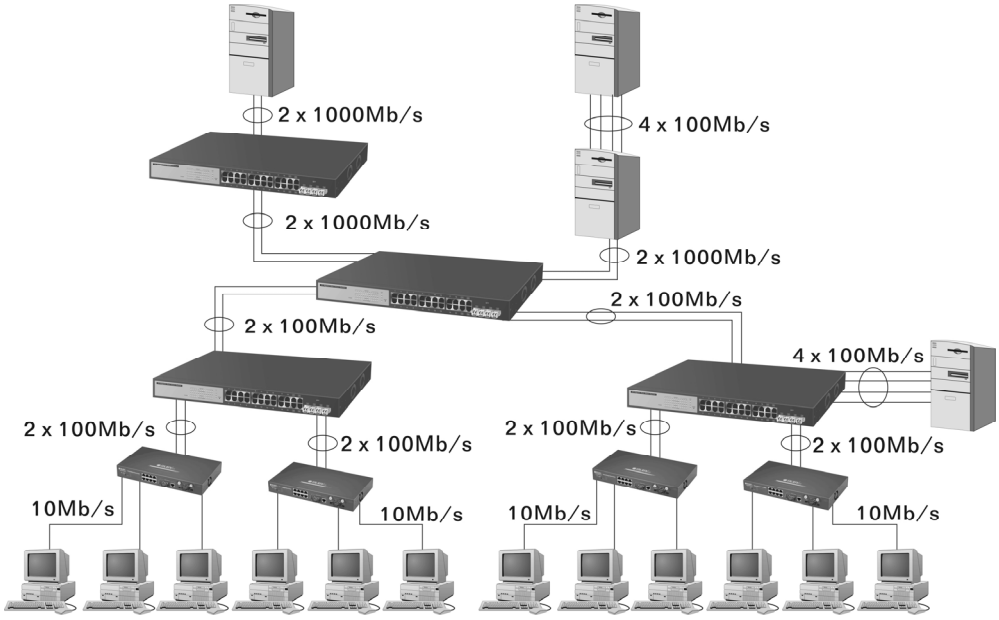


Fig. 3-10 Example of Link Aggregation Application

4. Operation of Web-based Management

This chapter instructs you how to configure and manage the 24-Port GbE Web Smart Switch through its web user interface and how to access and manage 20 10/100/1000Mbps TP Port and 4 Gigabit TP/SFP Fiber dual media port. The switch provides 20 fixed Gigabit Ethernet TP ports and four optional Gigabit dual media ports supporting either fiber or TP media. With this facility, you can easily access and monitor the statuses of all ports through any one port of the switch, including MIBs status, activity of each port, multicast traffic, and so on.

The default values of 24-Port GbE Web Smart Switch are listed in the table below:

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Password	admin

Table 4-1

After the 24-Port GbE Web Smart Switch being finished configuration, you can browse it by using the IP address you set up for it. For instance, type http://192.168.1.1 in the address row in a browser, it will show the following screen (see Fig.4-1) and ask you to key in password in order to login and access authentication. The default password is “admin”. For the first time to use, please enter the default password, then click the **<Apply>** button. The login process is now completed.

In the switch, it supports a simple user management function which only allows one administrator to configure the system at one time.

To optimize and obtain best view on screen, we recommend you use Microsoft IE and have the resolution set to 1024x768.

Here is the whole function tree of the web user interface and we will go through it in this chapter.

Fig. 4-1

4-1. Web Management Home Overview

After you login, the switch shows you the system status information as Fig. 4-2. This is the default page and it displays you with the basic information of the system, including “Switch Status”, “TP Port Status”, “Fiber Port Status”, “Aggregation”, “VLAN”, “Mirror”, “SNMP”, and “Maximum Packet Length”. With this information, you will know the software version used, MAC address, how many good and so on. For more details, please refer to Section 4-4-1.

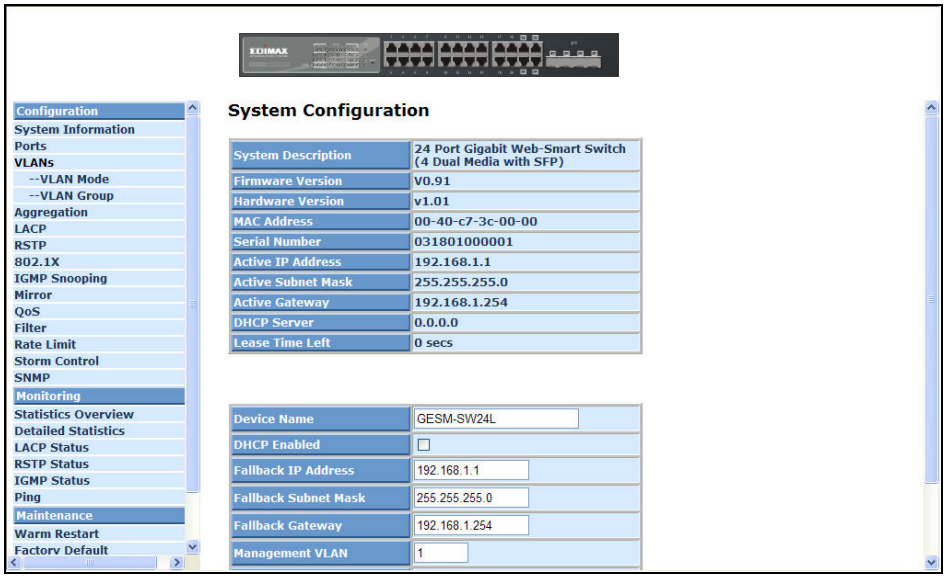
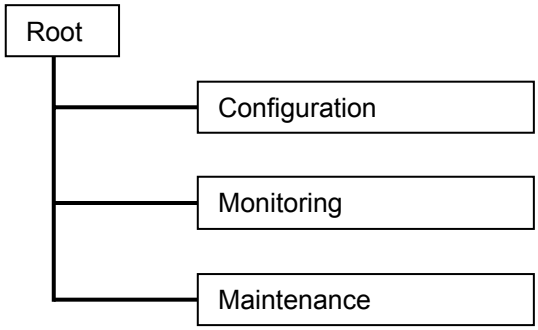


Fig. 4-2

• The Information of Page Layout

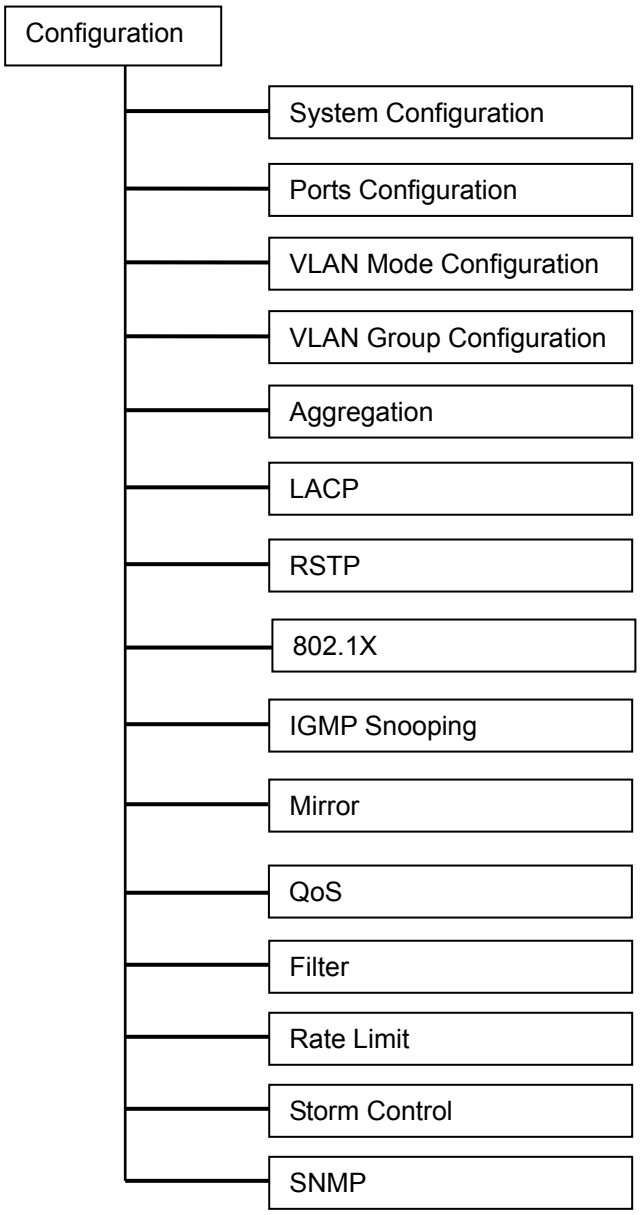
— On the top, it shows the front panel of the switch. In the front panel, green LEDs on to show linked ports in function; for unlinked ports the LEDs will be OFF. For the optional modules, the slot will show only a cover plate if no module exists. On the other hand, it will show a module if one presents. The image of module varies depends on the one you inserted. Again, if disconnected, the port will show just dark, if linked, green.

— On the left side, the main tree menu of the web user interface is listed. According to the function name in boldface, all functions can be divided into three parts, including “Configuration”, “Monitoring” and “Maintenance”. The functions of each folder are described in its corresponded section respectively. As to the function names in normal type are the sub-functions. When clicking it, the function is performed. The following list is the main function tree for the web user interface.



4-2. Configuration

Fifteen functions, including System Configuration, Ports Configuration, VLAN Mode Configuration, VLAN Group Configuration, Aggregation, LACP, RSTP, 802.1X, IGMP Snooping, Mirror, QoS, Filter, Rate Limit, Storm Control and SNMP are contained in this function folder for system and network management. Each of them will be described in detail orderly in the following sections.



4-2-1. System Configuration

System configuration is one of the most important configurations in the switch. Without proper settings, network administrator will not be able to manage or view the status of this device.The switch supports manual IP address setting.

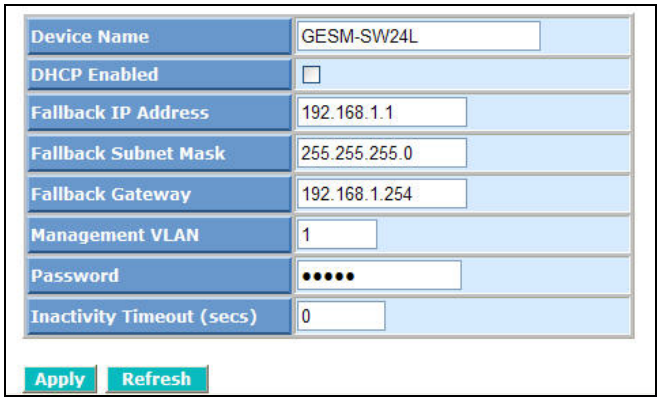


Fig. 4-3

Function name:

System Configuration

Function description:

Show system description, firmware version, hardware version, MAC address, serial number, active IP address, active subnet mask, active gateway, DHCP server and Lease time left.

Set device name, DHCP enable, fallback IP address, fallback subnet mask, fallback gateway, management VLAN, password and inactivity timeout.

Parameter description:

System Description:

The simple description of this switch.

Firmware Version:

The firmware version of this switch.

Hardware Version:

The hardware version of this switch.

MAC Address:

It is the Ethernet MAC address of the management agent in this switch.

Serial Number:

The serial number is assigned by the manufacturer.

Active IP Address:

Show the active IP address of this switch.

Active Subnet Mask:

Show the active subnet mask of this switch.

Active Gateway:

Show the active gateway of this switch.

DHCP Server:

Show the IP address of the DHCP server.

Default: 0.0.0.0

Lease Time Left:

Show the lease time left of DHCP client.

Device Name:

Set a special name for this switch. Up to 16 characters are allowed in this parameter. Any alphanumeric character and null are acceptable.

Default: Giga Switch

DHCP Enabled:

Enable DHCP snooping, Just tick the check box (☑) to enable it.

Default: disable

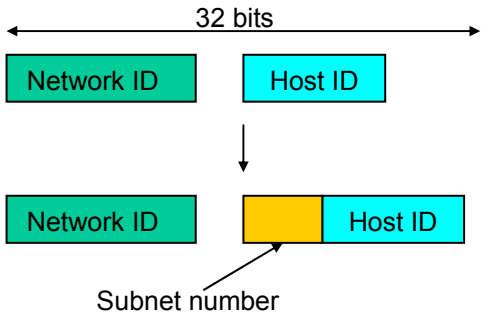
Fallback IP Address:

Users can configure the IP settings and fill in new values. Then, click **<Apply>** button to update.

Default: 192.168.1.1

Fallback Subnet Mask:

Subnet mask is made for the purpose to get more network addresses because any one IP device in a network must own its IP address, composed of Network address and Host address, otherwise it can't communicate with other devices on the network. But unfortunately, the network classes A, B, and C are all too large to fit for almost all networks, hence, subnet mask is introduced to solve this problem. Subnet mask uses some bits from host address and makes an IP address looked Network address, Subnet mask number and host address. It is shown in the following figure. This reduces the total IP number of a network able to support, by the amount of 2 to power of the bit number of subnet number (2^(bit number of subnet number)).



Subnet mask is used to set the subnet mask value, which should be the same value as that of the other devices resided in the same network it attaches.

For more information, please also see the Section 2-1-4 “IP Address Assignment” in this manual.

Default: 255.255.255.0

Fallback Gateway:

Set an IP address for a gateway to handle those packets that do not meet the routing rules predefined in the device. If a packet does not meet the criteria for other pre-defined path, it must be forwarded to a default router on a default path. This means any packet with undefined IP address in the routing table will be sent to this device unconditionally.

Default: 192.168.1.254

Management VLAN:

Show the management VLAN number.

Password:

Set a password for this switch. Up to 16 characters are allowed in this parameter. Any alphanumeric character is acceptable.

Default: admin

Inactivity Timeout(secs):

Set the auto-logout timer. The valid value is 0 ~ 60 in the unit of minute and a decimal point is not allowed. The value 0 means auto-logout timer is disabled.

Default: 0

4-2-2. Port Configuration

Function name:

Ports Configuration

Function description:

Ports Configuration is applied to change the settings of each port. In this configuration function, you can set/reset the following parameters, Mode and Flow Control. All of them are described in details below.

Parameter description:

Enable Jumbo Frames:

This function supports jumbo frames of up to 9600 bytes, Just tick the check box (☑) to enable it.

Default: disable

Link:

Show link status of this port.

Mode:

Set the speed and duplex of the port. If the media is 1Gbps fiber, there are three modes to choose: Auto Speed, 1000 Full and Disable. If the media is TP, the Speed/Duplex is comprised of the combination of speed mode, 10/100/1000Mbps, and duplex mode, full duplex and half duplex. The following table summarizes the function the media supports.

Media type	NWay	Speed	Duplex
1000M TP	ON/OFF	10/100/1000M	Full for all, Half for 10/100
1000M Fiber	ON/OFF	1000M	Full

In Auto Speed mode, no default value. In Forced mode, default value depends on your setting.

Flow Control:

You can Just tick the check box (☑) to enable flow control. If flow control is set Enable, both parties can send PAUSE frame to the transmitting device(s) if the receiving port is too busy to handle. When it is set Disable, there will be no flow control in the port. It drops the packet if too much to handle.

Default: Disable

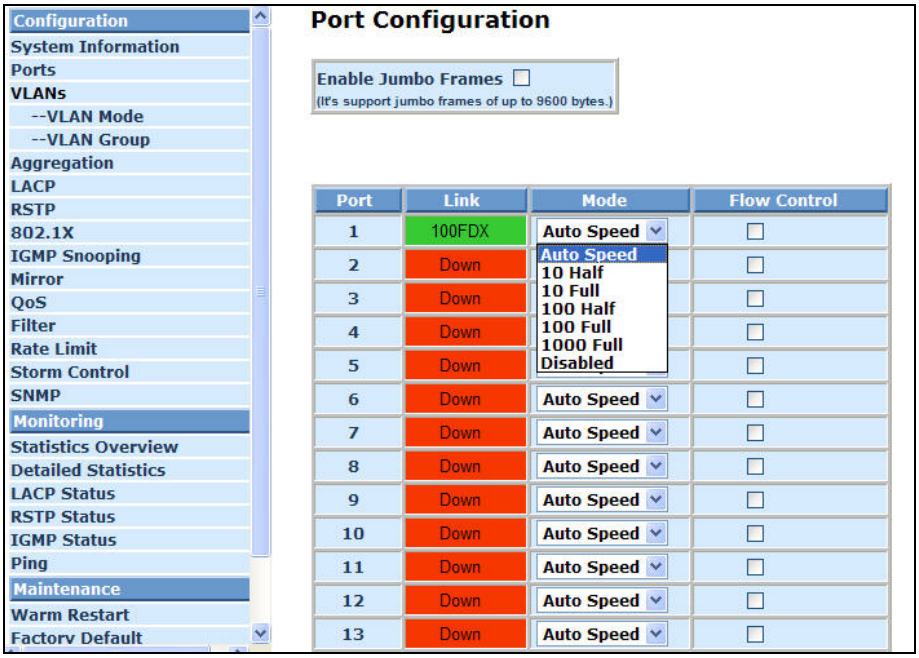


Fig. 4-4 Port Configuration

4-2-3. VLAN Mode Configuration

The switch supports Port-based VLAN and Tag-based VLAN (802.1q). Support 24 active VLANs and VLAN ID 1~4094. VLAN configuration is used to partition your LAN into small ones as your demand. Properly configuring it, you can gain not only improved security and increased performance but also greatly reduced VLAN management.

Function name:

VLAN Mode Setting

Function description:

The VLAN Mode Selection function includes four modes: Port-based, Tag-based, Metro mode or Disable. You can choose one of them by pulling down list and pressing the **<Downward>** arrow key. Then, click **<Apply>** button, the settings will be in effect immediately.

Parameter description:

VLAN Mode:

Port-based:

Port-based VLAN is defined by port. Any packet coming in or outgoing from any one port of a port-based VLAN will be accepted. No filtering criterion applies in port-based VLAN. The only criterion is the physical port you connect to. For example, for a port-based VLAN named PVLAN-1 contains port members Port 1&2&3&4. If you are on the port 1, you can communicate with port 2&3&4. If you are on the port 5, then you cannot talk to them. Each port-based VLAN you built up must be assigned a group name. This switch can support up to maximal 24 port-based VLAN groups.

Tag-based:

Tag-based VLAN identifies its member by VID. This is quite different from port-based VLAN. If there are any more rules in ingress filtering list or egress filtering list, the packet will be screened with more filtering criteria to determine if it can be forwarded. The switch supports supplement of 802.1q. For more details, please see the section VLAN in Chapter 3.

Each tag-based VLAN you built up must be assigned with a VLAN name and a VLAN ID. Valid VLAN ID is 1-4094. User can create total up to 24 Tag VLAN groups.

Double-tag:

Double-tag mode belongs to the tag-based mode, however, it would treat all frames as the untagged ones, which means that tag with PVID will be added into all packets. Then, these packets will be forwarded the same way as Tag-based VLAN. So, the incoming packets with tags will become the double-tag ones.

Metro Mode:

The Metro Mode is a quick configuration VLAN environment method on Port-based VLAN. It will create 21, 22, 23 or 24 Port-based VLAN groups.

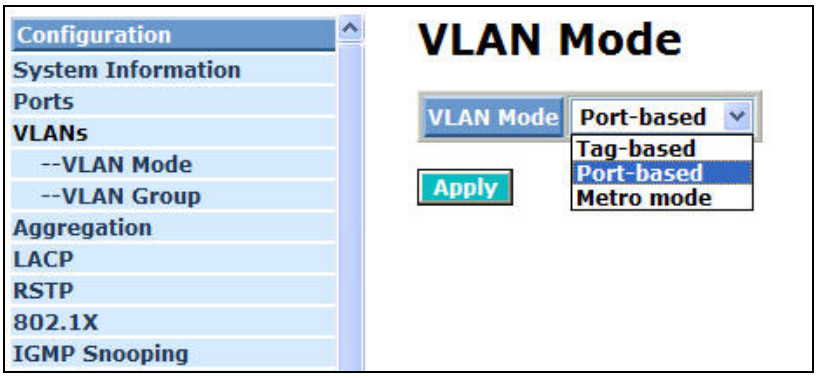


Fig. 4-5 Select VLAN Mode

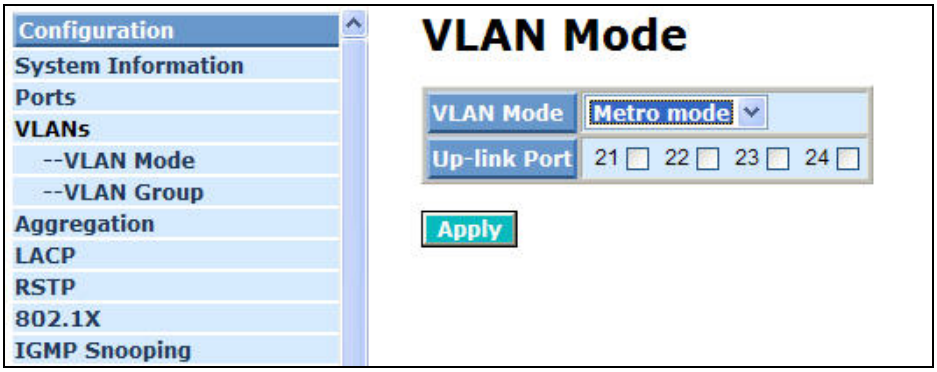


Fig. 4-6 Metro mode

4-2-4. VLAN Group Configuration

Function name:

VLAN Group Configuration

Function description:

It shows the existing information of VLAN Groups List and the maintenance that can be done to them, i.e. modify and delete. User also can add a new VLAN group by inputting a new VLAN name and VLAN ID.

If you are in port-based VLAN, it will just show the ID and Member of the existed port-based VLAN group. If you are in tag-based VLAN, it will show the ID, VID, Member of the existed tag-based VLAN group. The switch can store the configuration of port-based VLAN and tag-based VLAN separately. When you choose one of VLAN mode, the switch will bring you the responded VLAN configuration which keeps the default data. You can easily create or delete a VLAN group by pressing **<Add>** or **<Delete>** function buttons, or click the Group ID directly to edit it.

Parameter description:

ID (Group ID):

When you want to edit a VLAN group, you must select the Group ID field. Then, you will enter Tag Base VLAN Group Setting or Port Base VLAN Group Setting page, which depends on your VLAN mode selection.

VID:

VLAN identifier. Each tag-based VLAN group has a unique VID. It appears only in tag-based mode.

Member:

In modify function this is used to enable or disable a port if it is a member of the new added VLAN, “Enable” means it is a member of the VLAN. Just tick the check box (☑) beside the port x to enable it.

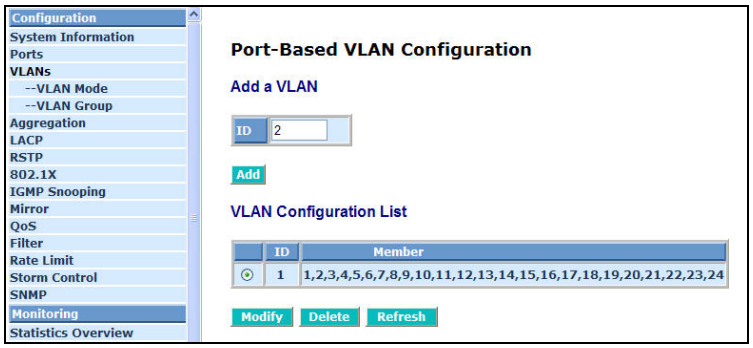


Fig. 4-7 Port-Based VLAN Configuration

Add Group:

Create a new port-based VLAN or tag-based VLAN, which depends on the VLAN mode you choose in VLAN mode function.

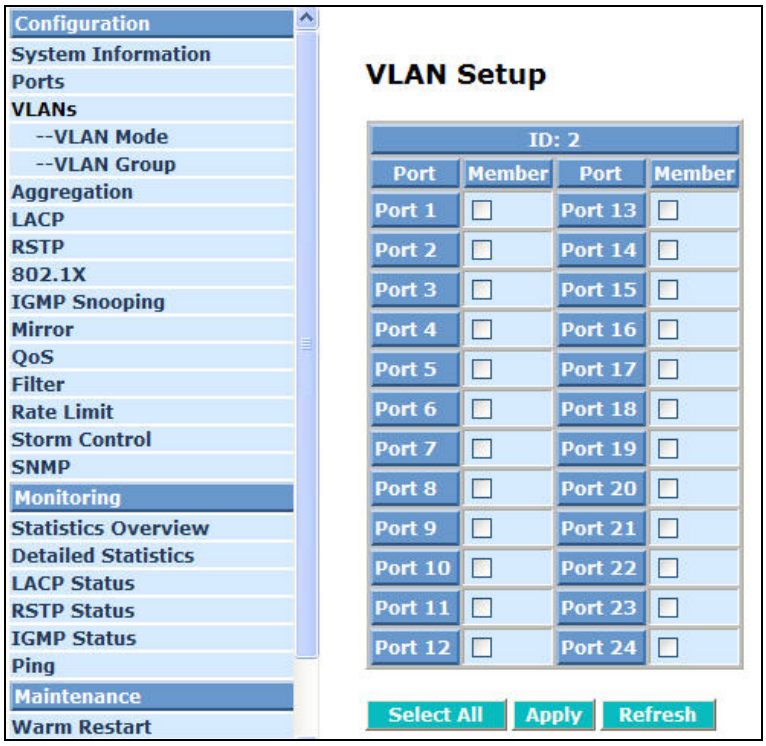


Fig. 4-8 Add or Remove VLAN Member

Delete Group:

Just tick the check box (☑) beside the ID, then press the **<Delete>** button to delete the group.

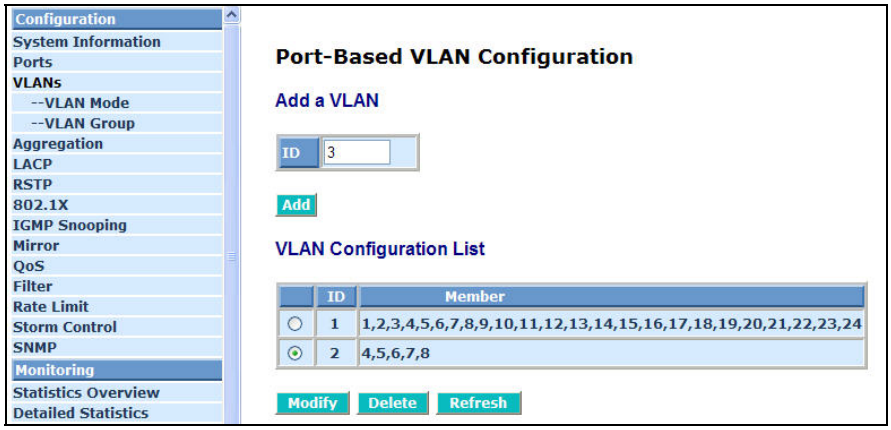


Fig. 4-9 Port-Based VLAN Configuration

4-2-5. Aggregation

The Aggregation (Port Trunking) Configuration is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex and the same MAC to be one single logical port, thus the logical port aggregates the bandwidth of these bundled ports This means you can apply your current Ethernet equipments to build the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, this logical port will have bandwidth of three times high as a single Fast Ethernet port.

Function name:

Aggregation Configuration

Function description:

Display the current setup of Aggregation Trunking. With this function, user is allowed to add a new trunking group or modify the members of an existed trunking group.

Parameter description:

Normal:

Set up the ports that do not join any aggregation trunking group.

Group 1~8:

Group the ports you choose together. Up to 12 ports can be selected for each group.

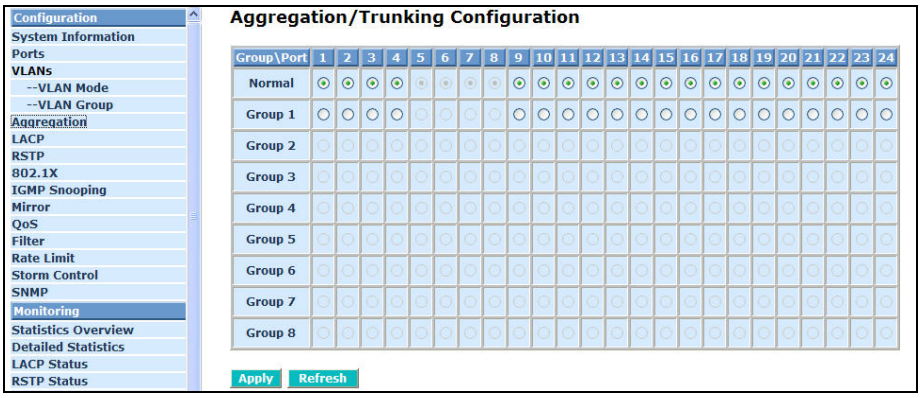


Fig. 4-10 Aggregation/Trunking Configuration

4-2-6. LACP

The switch supports the link aggregation IEEE802.3ad standard. This standard describes the Link Aggregate Control Protocol (LACP), which is a protocol that dynamically creates and manages trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an operational port fails, then one of the “standby” ports become operational without user intervention.

Function name:

LACP Port Configuration

Function description:

Enable or disable LACP protocol, user is allowed to set the aggregation key value.

Parameter description:

Protocol Enabled:

Just tick the check box (☑) to enable LACP protocol then press the **<Apply>** button to apply.

Key Value:

It’s key for an aggregation. This must be an integer value between 1 and 255 or auto selected by switch.

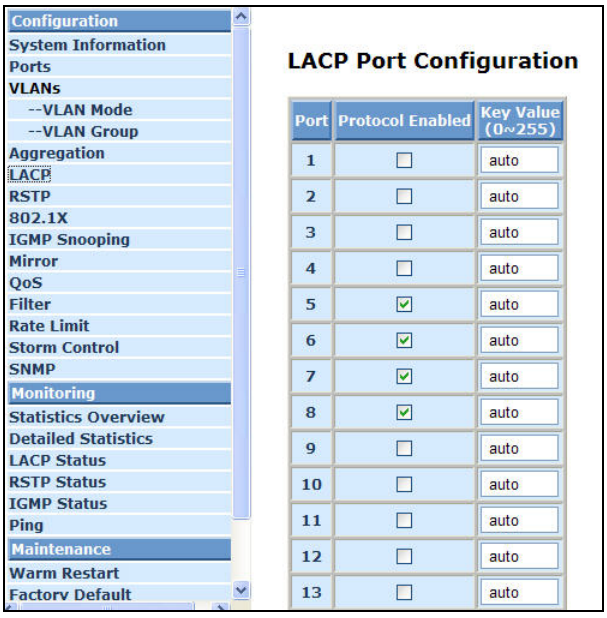


Fig. 4-11 LACP Port Configuration

4-2-7. RSTP

RSTP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a switch to interact with other RSTP – compliant switches in your network to ensure that only one path exists between any two stations on the network.

The switch allows you to create multiple STP configurations and assign ports to a specific tree.

Function name:

RSTP System Configuration

Function description:

This screen is used to display the RSTP system configuration and necessary parameters.

Parameter description:

System Priority:

System priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box.

The lower the numeric value you assign, the higher the priority for this system.

Default: 32768

Hello Time:

This is the time interval in seconds between BPDU configuration message generations by the root switch. The allowed range is 1 to 10 seconds.

Default: 2

Max Age:

This is the maximum time a switch can wait without receiving a BPDU before attempting to reconfigure. The allowed range is 6 to 40 seconds.

Default: 20

Forward Delay:

This is the maximum time (in seconds) a switch will wait before changing states. The general rule: 2 * (Forward Delay – 1) >= Max Age >= 2 * (Hello Time + 1)

Default: 15

Force version:

Select RSTP or STP protocol from the drop-down list box.

Function name:

RSTP Port Configuration

Function description:

Enable or disable RSTP protocol on the port which being selected and set path cost.

Parameter description:

Protocol Enabled:

Just tick the check box (☑) beside the port x to enable RSTP protocol, then press the **<Apply>** button to apply.

Edge:

Just tick the check box (☑) beside the port x to enable edge function.

Path Cost:

Path cost is the cost of transmitting a frame on to a LAN through that port. It is assigned according to the speed of the bridge. The slower the media, the higher the cost, user can select auto or set the rage from 1 to 200000000.

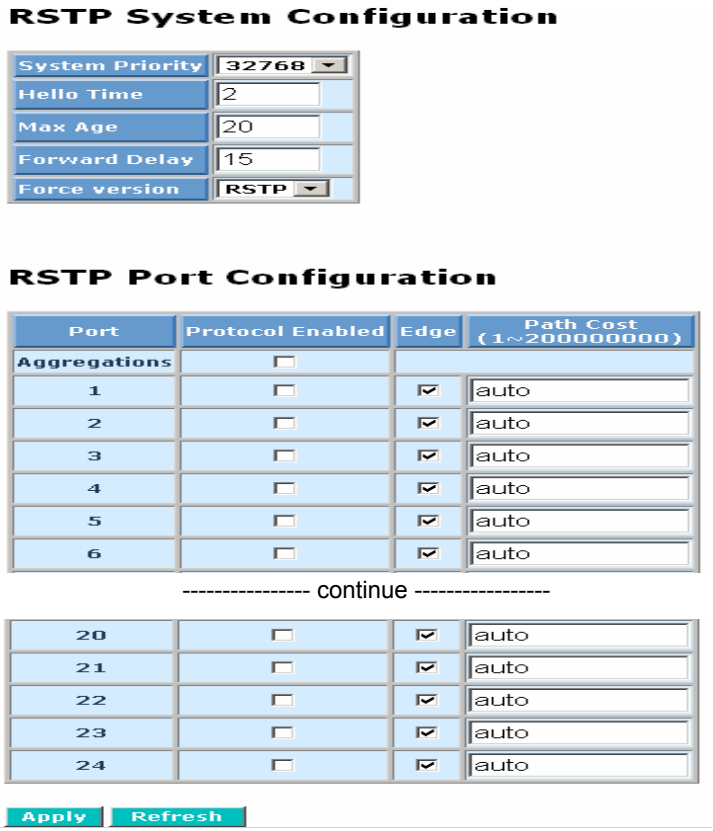


Fig. 4-12 RSTP Configuration

4-2-8. 802.1X

802.1x port-based network access control provides a method to restrict users to access network resources via authenticating user's information. This restricts users from gaining access to the network resources through a 802.1x-enabled port without authentication. If a user wishes to touch the network through a port under 802.1x control, he (she) must firstly input his (her) account name for authentication and waits for gaining authorization before sending or receiving any packets from a 802.1x-enabled port.

Before the devices or end stations accessing the network resources through the ports under 802.1x control, the devices or end stations connects to a controlled port by sending the authentication request to the authenticator, the authenticator passes the request to the authentication server to authenticate and verify, and the server tells the authenticator if the request get the grant of authorization for the ports.

According to IEEE802.1x, there are three components implemented. They are Authenticator, Supplicant and Authentication server shown in Fig. 4-13.

Supplicant:

It is an entity being authenticated by an authenticator. It is used to communicate with the Authenticator PAE (Port Access Entity) by exchanging the authentication message when the Authenticator PAE request is sent to it.

Authenticator:

An entity facilitates the authentication of the supplicant entity. It controls the state of the port, authorized or unauthorized, according to the result of authentication message exchanged between it and a supplicant PAE. The authenticator may request the supplicant to re-authenticate itself at a configured time period. Once start re-authenticating the supplicant, the controlled port keeps in the authorized state until re-authentication fails.

A port acting as an authenticator is thought to be two logical ports, a controlled port and an uncontrolled port. The controlled port can only pass the packets when the authenticator PAE is authorized, and on the other hand, the uncontrolled port will unconditionally pass the packets with PAE group MAC address, which has the value of 01-80-c2-00-00-03 and will not be forwarded by MAC bridge, at any time.

Authentication server:

A device provides authentication service, through EAP (Extensible Authentication Protocol), to an authenticator by using authentication credentials supplied by the supplicant to determine if the supplicant is authorized to access the network resource.

The overview of operation flow for the Fig. 4-13 is quite simple. When Supplicant PAE issues a request to Authenticator PAE, the Authenticator and Supplicant will exchange authentication message. Then, the Authenticator passes request to RADIUS server to verify. Finally, RADIUS server replies if the request is granted or denied.

While in the authentication process, the message packets encapsulated by Extensible Authentication Protocol over LAN (EAPOL), are exchanged between an authenticator PAE and a supplicant PAE. The Authenticator exchanges the message to authentication server using EAP encapsulation. Before successfully authenticating, the supplicant can only reach the authenticator to perform authentication message exchange or access the network from the uncontrolled port.

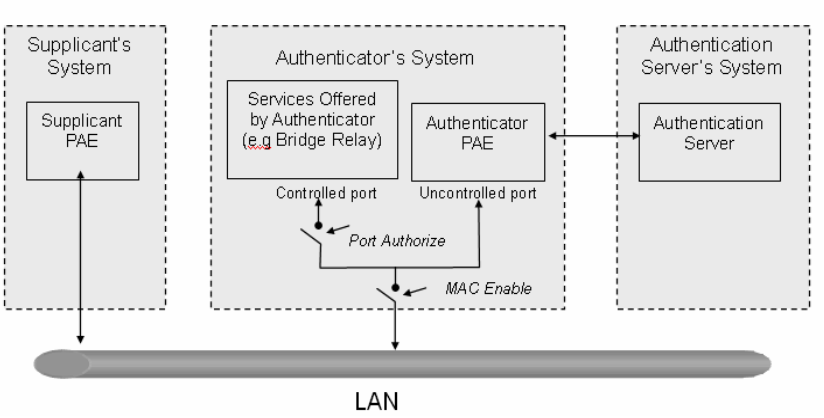


Fig. 4-13

In the Fig. 4-14, this is the typical configuration, a single supplicant, an authenticator and an authentication server. B and C is in the internal network, D is Authentication server running RADIUS, switch at the central location acts Authenticator connecting to PC A and A is a PC outside the controlled port, running Supplicant PAE. In this case, PC A wants to access the services on device B and C, first, it must exchange the authentication message with the authenticator on the port it connected via EAPOL packet. The authenticator transfers the supplicant's credentials to Authentication server for verification. If success, the authentication server will notice the authenticator the grant. PC A, then, is allowed to access B and C via the switch. If there are two switches directly connected together instead of single one, for the link connecting two switches, it may have to act two port roles at the end of the link: authenticator and supplicant, because the traffic is bi-directional.

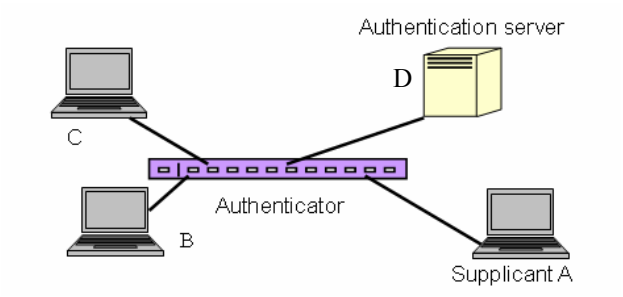


Fig. 4-14

Fig. 4-15 shows procedures of the 802.1x authentication. There are steps for the login process based on 802.1x port access control management. The protocol used on the right side is EAPOL and on the left side is EAP.

1. On the initial stage, the supplicant A is unauthenticated and a port on switch acting as an authenticator is in unauthorized state. So the access is blocked in this stage.

2. Initiating a session. Either authenticator or supplicant can initiate the message exchange. If supplicant initiates the process, it sends EAPOL-start packet to the authenticator PAE and authenticator will immediately respond EAP-Request/Identity packet.

3. The authenticator always periodically sends EAP-Request/Identity to the supplicant for requesting the identity it wants to be authenticated.

4. If the authenticator doesn't send EAP-Request/Identity, the supplicant will initiate EAPOL-Start the process by sending to the authenticator.

5. And next, the Supplicant replies an EAP-Response/Identity to the authenticator. The authenticator will embed the user ID into Radius-Access-Request command and send it to the authentication server for confirming its identity.

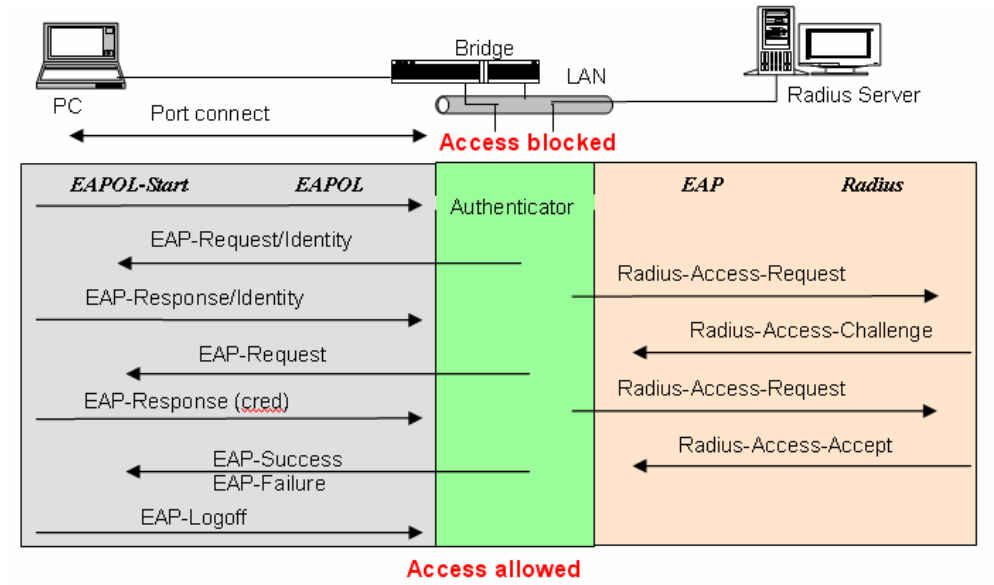
6. After receiving the Radius-Access-Request, the authentication server sends Radius-Access-Challenge to the supplicant and asks or user password via the authenticator PAE.

7. The supplicant will convert user password into the credential information, perhaps, in MD5 format and replies an EAP-Response with this credential information as well as the specified authentication algorithm (MD5 or OTP) to Authentication server via the authenticator PAE. As per the value of the type field in message PDU, the authentication server knows which algorithm should be applied to authenticate the credential information, EAP-MD5 (Message Digest 5) or EAP-OTP (One Time Password) or other else algorithm.

8. If the user ID and password is correct, the authentication server will send a Radius-Access-Accept to the authenticator. If not correct, the authentication server will send a Radius-Access-Reject.

9. When the authenticator PAE receives a Radius-Access-Accept, it will send an EAP-Success to the supplicant. At this time, the supplicant is authorized and the port connected to the supplicant and under 802.1x control is in the authorized state. The supplicant and other devices connected to this port can access the network. If the authenticator receives a Radius-Access-Reject, it will send an EAP-Failure to the supplicant. This means the supplicant is failed to authenticate. The port it connects is in the unauthorized state, the supplicant and the devices connected to this port won't be allowed to access the network.

10. When the supplicant issue an EAP-Logoff message to Authentication server, the port you are using is set to be unauthorized..



The 802.1X “Enabled” is the type of authentication supported in the switch. In this mode, for the devices connected to this port, once a supplicant is authorized, the devices connected to this port can access the network resource through this port.

802.1x Port-based Network Access Control function supported by the switch is a little bit more complex, for it just supports basic “Enabled” mode, which can distinguish the device’s MAC address and its VID. The following table is the summary of the combination of the authentication status and the port status versus the status of port mode, set in 802.1x Port mode, port control state, set in 802.1x port setting. Here Entry Authorized means MAC entry is authorized.

Port Mode	Port Control	Authentication	Port Status
Disable	Don’t Care	Don’t Care	Port Uncontrolled
Enabled	Auto	Successful	Port Authorized
Enabled	Auto	Failure	Port Unauthorized
Enabled	ForceUnauthorized	Don’t Care	Port Unauthorized
Enabled	ForceAuthorized	Don’t Care	Port Authorized

Function name:

802.1X Configuration

Function description:

This function is used to configure the global parameters for RADIUS authentication in 802.1x port security application. *Parameter description:*

Mode:

Enable or disable 802.1X function.

RADIUS IP:

RADIUS server IP address for authentication.

Default: 0.0.0.0

RADIUS UDP Port:

The port number to be used communicate with RADIUS server for the authentication service. The valid value ranges 1-65535.

Default port number is 1812.

RADIUS Secret:

The secret key between authentication server and authenticator. It is a string with the length of 1 – 15 characters. The character string may contain upper case, lower case and 0-9. It is character case sensitive. A blank in between any two characters is not allowed.

Default: None

Admin State:

This is used to set the operation mode of authorization. There are three types of operation mode supported, Force Unauthorized, Force Authorized and Auto.

- Force Unauthorized:

  The controlled port is forced to hold in the unauthorized state.

- Force Authorized:

  The controlled port is forced to hold in the authorized state.

- Auto:

  The controlled port is set to be in authorized state or unauthorized state depends on the result of the authentication exchange between the authentication server and the supplicant.

Default: Force Authorized

Port State:

Show the port status of authorization.

Re-authenticate:

Specify if subscriber has to periodically re-enter his or her username and password to stay connected to the port.

Re-authenticate All:

Re-authenticate for all ports in at once.

Force Reinitialize:

Force the subscriber to reinitialize connection to the port.

Force Reinitialize All:

Force Reinitialize for all ports at once.

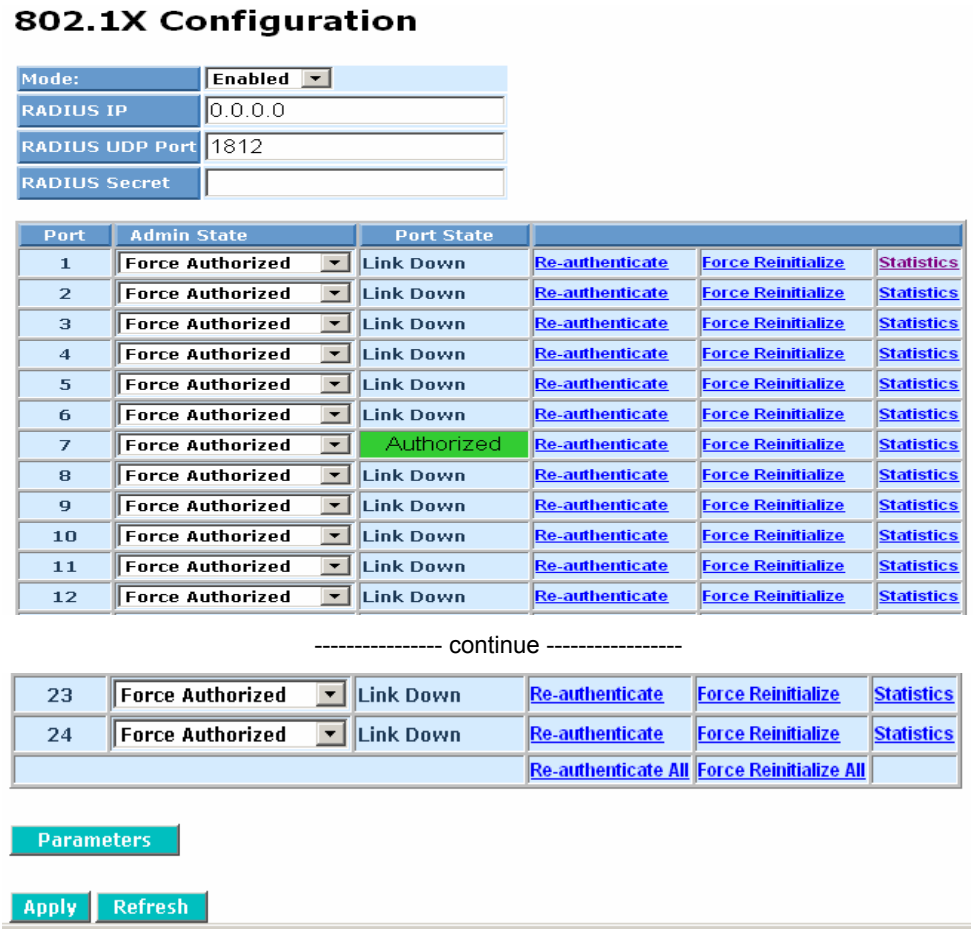


Fig. 4-16 802.1X Configuration

Statistics:

Choose the port which you want to show of 802.1X statistics, the screen include Authenticator counters, backend Authenticator counters, dot1x MIB counters and Other statistics.

Press the **<Refresh>** button will fresh the screen and you can see the newer counters.

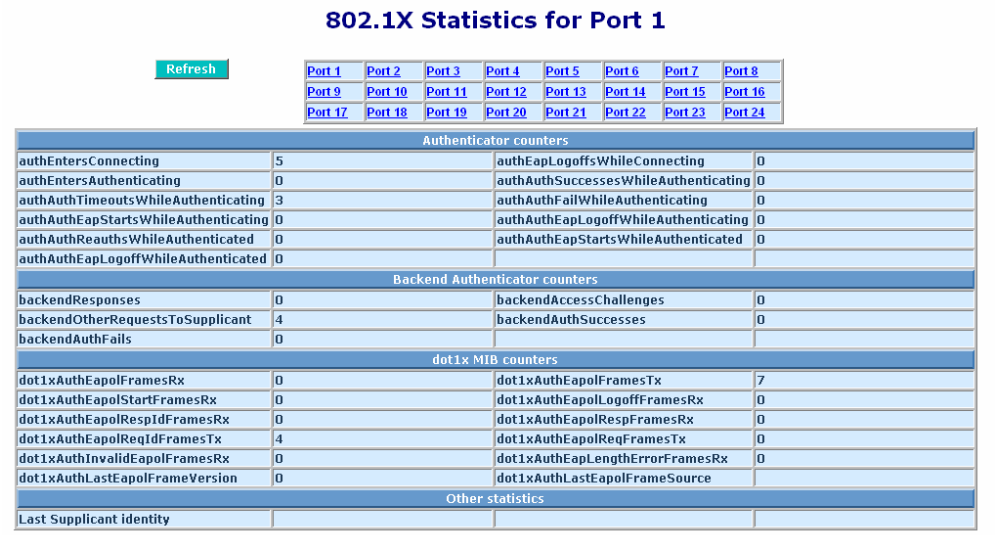


Fig. 4-17 802.1X Statistics

Function name:

802.1x Parameters

Function description:

In here, user can enable or disable Reauthentication function and specify how often a client has to re-enter his or her username and password to stay connected to the port.

Parameter description:

Reauthentication Enabled:

Choose whether regular authentication will take place in this port.

Default: disable

Reauthentication Period (1-65535 s):

A non-zero number seconds between the periodic re-authentication of the supplicant.

Default: 3600

EAP timeout ((1-255 s):

A timeout condition during in exchange between the authenticator and the supplicant. The valid range: 1 –255.

Default: 30 seconds

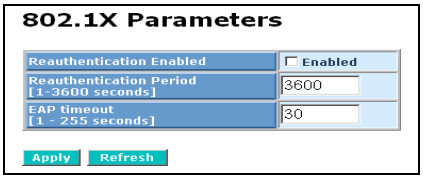


Fig. 4-18 802.1X Parameters

4-2-9 IGMP Snooping

Function name:

IGMP Snooping Configuration

Function description:

IGMP snooping enable group multicast traffic to only be forwarded to ports that are members of that group; thus allowing you to significantly reduce multicast traffic passing through the switch. All the functions should press **<Apply>** button to start up after you tick the check box.

Parameter description:

IGMP Enabled:

Just tick the check box (☑) to enable this function.

Default: disable

Router Ports:

Just tick the check box (☑) beside the port x to enable router ports, then press the **<Apply>** button to start up.

Default: none

Unregistered IGMP Flooding enabled:

Just tick the check box (☑) to enable this function.

Default: enable

VLAN ID:

Once the IGMP Enable mode is selected, it will list the VLAN ID number.

IGMP Snooping Enabled:

After IGMP Enabled function start up, user can tick the check box (☑) to enable this function.

Default: enable

IGMP Querying Enabled:

After IGMP Enabled function start up, user can tick the check box (☑) to enable this function.

Default: enable

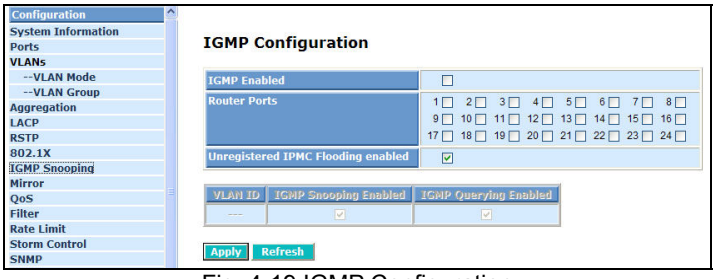


Fig. 4-19 IGMP Configuration

4-2-10. Mirror Configuration

Function name:

Mirror Configuration

Function description:

Mirror Configuration is to monitor the traffic of the network, this switch supports one port mirror multi ports. For example, we assume that Port A and Port B are Source Ports and Port C is Mirror Port respectively. The traffic passed by Port A and Port B will be copied to Port C for monitoring.

Parameter description:

Source Port:

Set up the port for being monitored. Just tick the check box (☑) beside the port x and valid port is Port 1~24.

Mirror Port:

Use the drop-down menu to select a mirror port.

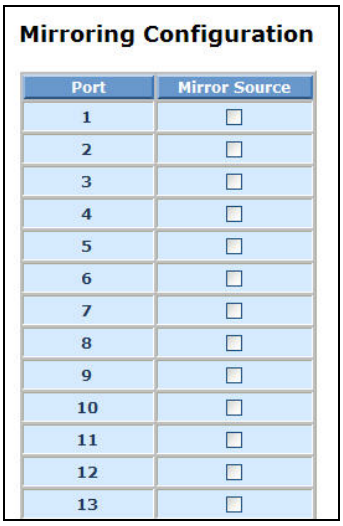


Fig. 4-20 Mirror ports configuration

4-2-11. QoS(Quality of Service) Configuration

The switch offers powerful QoS function. This function supports VLAN-tagged priority that can make precedence of 8 priorities, and DSCP(Differentiated Services Code Point) on Layer 3 of network framework.

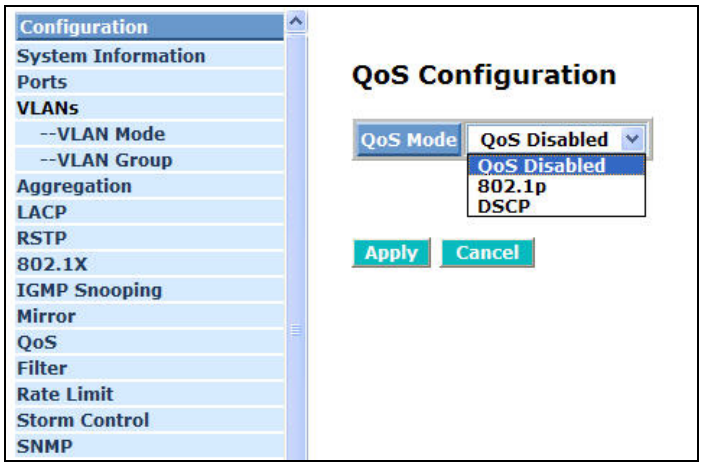


Fig. 4-21 QoS Configuration

Function name:

QoS Configuration

Function description:

When you want to use QoS function, please select QoS Mode through the drop-down menu in advance you can choose from 802.1p Priority or DSCP Priority to take effect. In this function, you can disable QoS Mode and choose any other Priority Control and enable it, such as 802.1p and DSCP. The switch only supports Strict Priority; and high priority queue is always passed first.

Function name:

Prioritize Traffic

Function description:

Five kinds of default values. The user can select from custom, or all low priority, or all normal priority, or all medium priority, or all high priority for QoS default value.

Function name:

802.1p Setting

Function description:

This function will affect the priority of VLAN tag. Based on priority of VLAN tag, it can arrange 0~7 priorities, Priorities can map up to 4 queues of the switch (low, normal, medium, high) and possess different bandwidth distribution according to your weight setting.

Parameter description:

802.1p Priority Mapping:

Each Priority can select any level of Queue. In Default, Priority 0 is mapping to Queue normal, Priority 1 is mapping to Queue low, Priority 2 is mapping to Queue low, Priority 3 is mapping to Queue normal, Priority 4 is mapping to Queue medium, Priority 5 is mapping to Queue medium, Priority 6 is mapping to Queue high, and Priority 0 is mapping to Queue high.

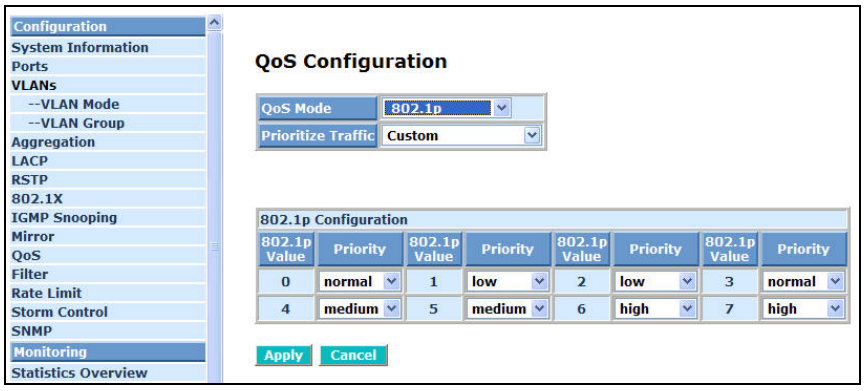


Fig. 4-22 802.1p Setting

Function name:

DSCP Setting

Function description:

In the late 1990s, the IETF redefined the meaning of the 8-bit SERVICE TYPE field to accommodate a set of differentiated services (DS). Under the differentiated services interpretation, the first six bits comprise a codepoint, which is sometimes abbreviated DSCP, and the last two bits are left unused.

DSCP can form total 64 (0~63) kinds of Traffic Class based on the arrangement of 6-bit field in DSCP of the IP packet. In the switch, the user is allowed to set up these 64 kinds of Classes that belong to any level of queue (low, normal, medium, high).

Parameter description:

DSCP Priority Mapping:

64 kinds of priority traffic as mentioned above, the user can set up any level of Queue (low, normal, medium, high). In default, Priority 0~63 are mapped to Queue high.

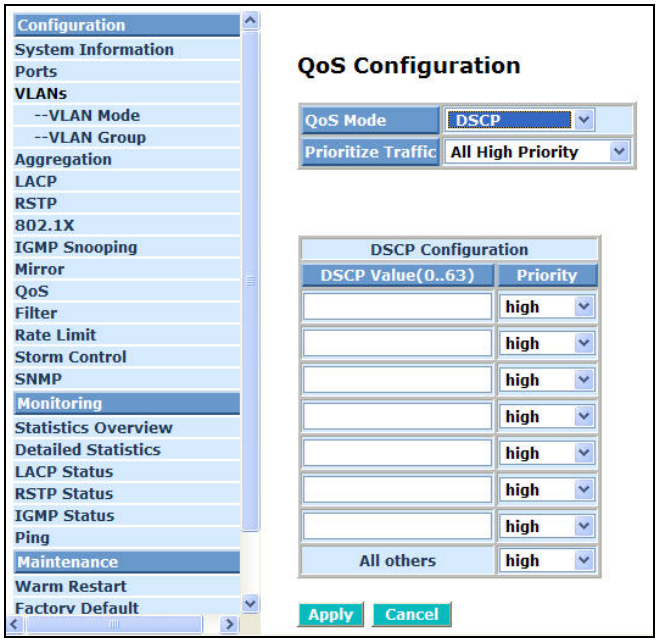


Fig. 4-23 DSCP Setting

4-2-12 Filter

Function name:

Filter Configuration

Function description:

This function can set management's source IP Address to each port, simple and raise safety. After completing the function's setting, press **<Apply>** button to have this function in effect.

Parameter description:

Source IP Filter:

Mode:

There are three types of modes in this drop-down menu. Default is disabled.

Disabled:

Allow users from all IP address to log in to this switch and manage it.

Static:

Only the user from the IP Address set by administrator is allowed to login to this switch and manage it..

DHCP:

Allow the user from an IP Address given by the DHCP server to login to this switch and manage it.

IP Address:

Setting up the IP Address, it can be one IP Address or a LAN.

IP Mask:

Setting up the IP Subnet Mask necessary for the IP Address.

DHCP Server Allowed:

Just tick the check box (☑) under the port x to allow the DHCP Server giving out an IP address; and valid ports are 1~24.

Default: enable

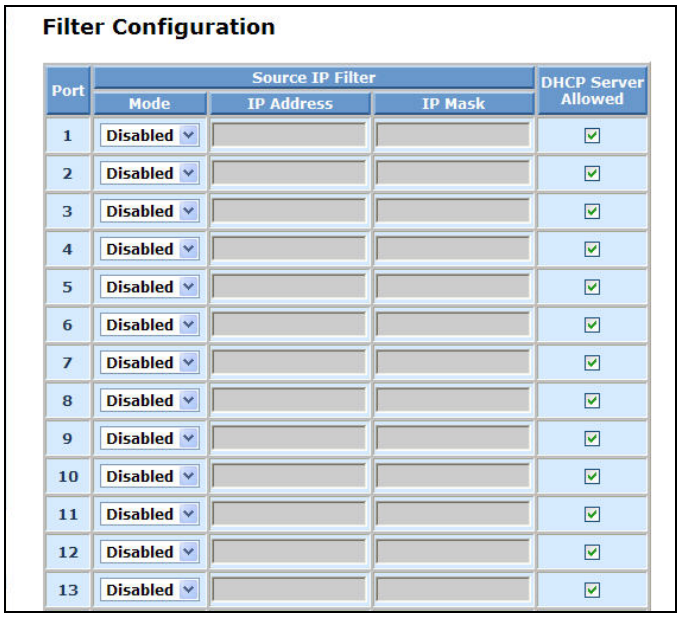


Fig. 4-24 Filter Configuration

4-2-13 Rate Limit

Function name:

Ingress and Egress Bandwidth Setting

Function description:

Ingress and Egress Bandwidth Setting function is used to set up the limit of Ingress or Egress bandwidth for each port.

Parameter description:

Ingress:

Set up the limit of Ingress bandwidth for the port you choose. Incoming traffic will be discarded if the rate exceeds the value you set up in Data Rate field. Pause frames are also generated if flow control is enabled. The format of the packet limits to unicast, broadcast and multicast. Valid value of Port 1~24 ranges from 128~3968 kbps.

Default: No Limit

Egress:

Set up the limit of Egress bandwidth for the port you choose. Outgoing traffic will be discarded if the rate exceeds the value you set up in Data Rate field. Pause frames are also generated if flow control is enabled. The format of the packet limits to unicast, broadcast and multicast. Valid value of Port 1~24 ranges from 128~3968 kbps.

Default: No Limit

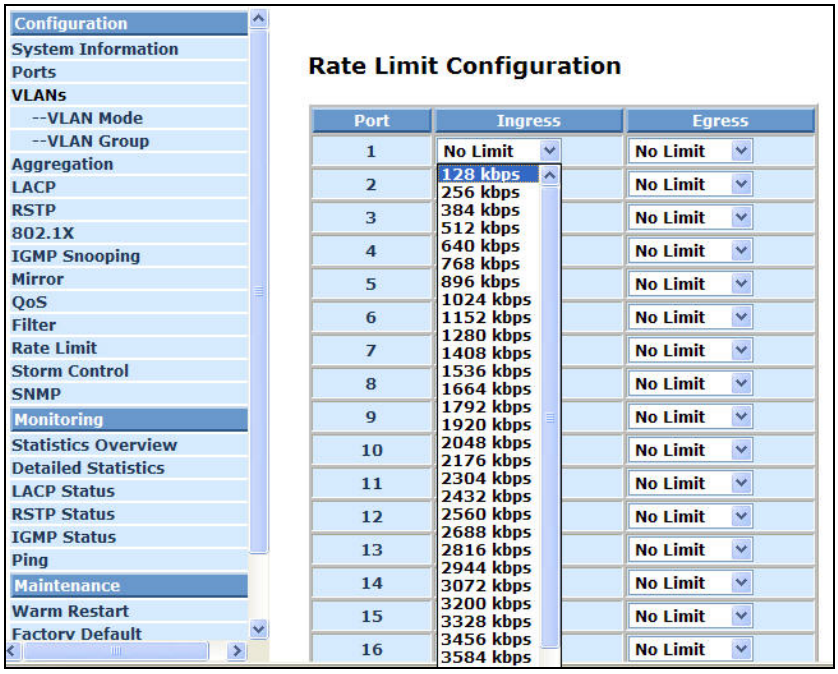


Fig. 4-25 Rate Limit Configuration

4-2-14 Storm Control

Function name:

Storm Control

Function description:

Storm Control is used to block unnecessary frames of the multicast and broadcast that would have reduced the switch's performance. When the frames of multicast or broadcast are over the rate and Strom Control is enabled, the frames that exceed the determined rate can be dropped.

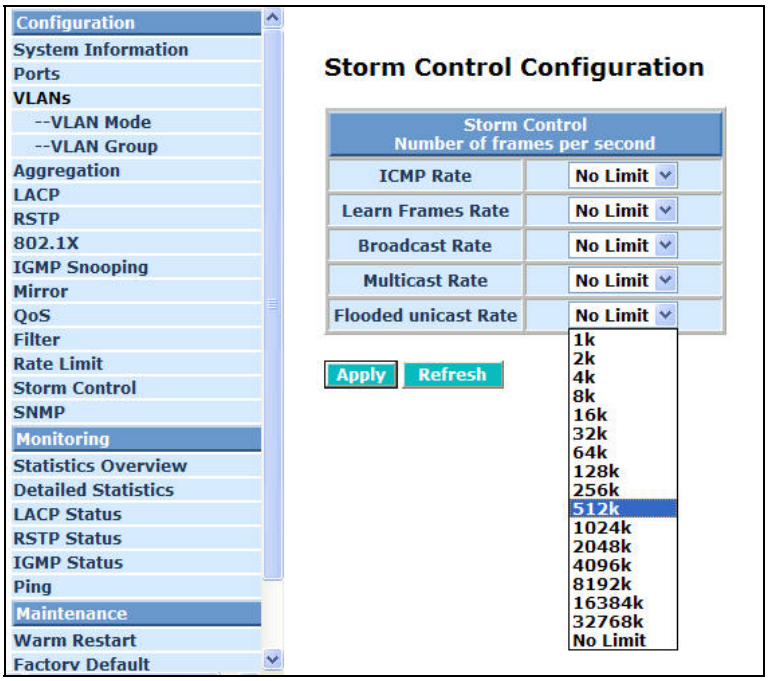


Fig.4-26 Storm Control Configuration

Parameter description:

ICMP Rate:

To enable the ICMP Storm capability. The user can use drop-down menu to select number of frames. Default is No Limit. The setting range is 1k~1024k per second.

Learn Frames Rate:

To enable the Learn Frames Storm capability. The user can use drop-down menu to select number of frames. Default is No Limit. The setting range is 1k~1024k per second.

Broadcast Rate:

To enable the Broadcast Storm capability. The user can use drop-down menu to select number of frames. Default is No Limit. The setting range is 1k~1024k per second.

Multicast Rate:

To enable the Multicast Storm capability. The user can use drop-down menu to select number of frames. Default is No Limit. The setting range is 1k~1024k per second.

Flooded unicast Rate:

To enable the Flooded unicast Storm capability. The user can use drop-down menu to select number of frames. Default is No Limit. The setting range is 1k~1024k per second.

NOTE:

After completing the function's setting, press **<Apply>** button to have this function taken effect.

4-2-15 SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. A SNMP agent is running on the switch to response the request issued by SNMP manager.

Basically, it is passive except issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP "Enable", the SNMP agent will be started up. All supported MIB OIDs, including RMON MIB, can be accessed via the SNMP manager. If the field SNMP is set "Disable", the SNMP agent will be de-activated. The related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

Function name:

SNMP Configuration

Function description:

This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP. A SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So, both parties must have the same community name. Once completing the setting, click **<Apply>** button, the setting takes effect.

Parameters description:

SNMP enable:

The term SNMP enable here is used to activate or de-activate SNMP. Default is disableing.

Get/Set/Trap Community:

Community name is used as password for authenticating if the requesting network management unit belongs to the same community group. If they both don't have the same community name, they don't belong to the same group. Hence, the requesting network management unit can not access the device with different community name via SNMP protocol. Only if they both have the same community name, they can talk each other.

Community name is user-definable with a maximum length of 15 characters and is case sensitive. It is not allowed to put any blank in the community name string. Any printable character is allowed.

The community name for each function works independently. Each function has its own community name. Say, the community name for Read only works for Read function and can't be applied to other function such as Write and Trap.

Default SNMP function: Disable

Default community name for Get: public

Default community name for Set: private

Default community name for Trap: public

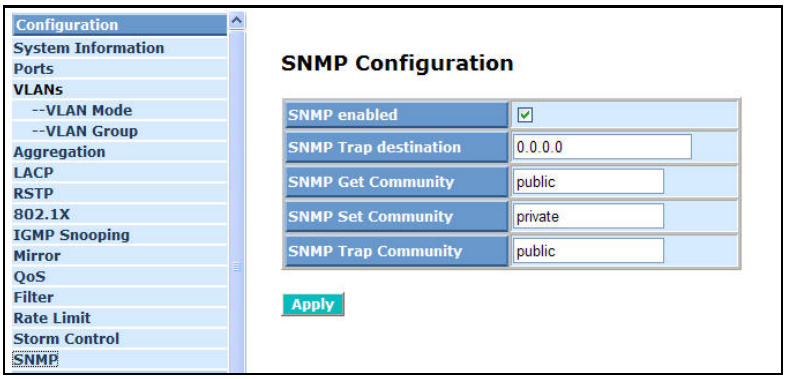
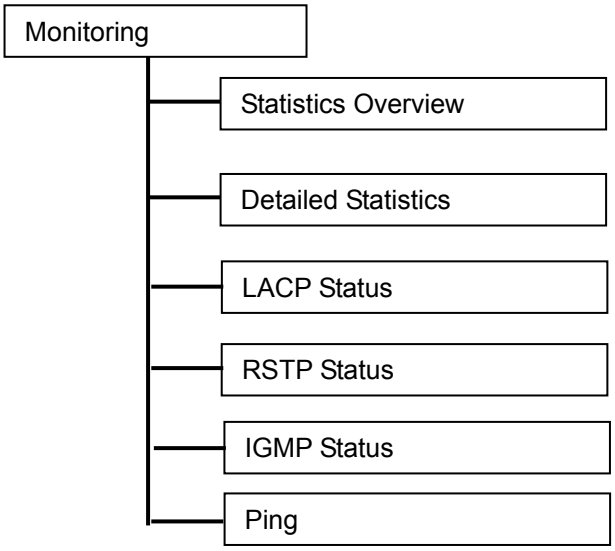


Fig. 4-27 SNMP Configuration

4-3. Monitoring

There are six functions under in the monitoring function.



4-3-1. Statistics Overview

The function of Statistics Overview collects any information and provides the counting summary about the traffic of the port, no matter the packet is good or bad.

In the Fig. 4-25, the window can show all ports' counter information at the same time. If the counting overflows, the counter will be reset the counting will restart.

Function name:

Statistics Overview

Function description:

Display the summary counting of each port's traffic, including Tx Bytes, Tx Frames, Rx Bytes, Rx Frames, Tx Errors and Rx Errors.

Parameters description:

Tx Bytes:

Total transmitted bytes.

Tx Frames:

The counting number of the packet transmitted.

Rx Bytes:

Total received bytes.

Rx Frames:

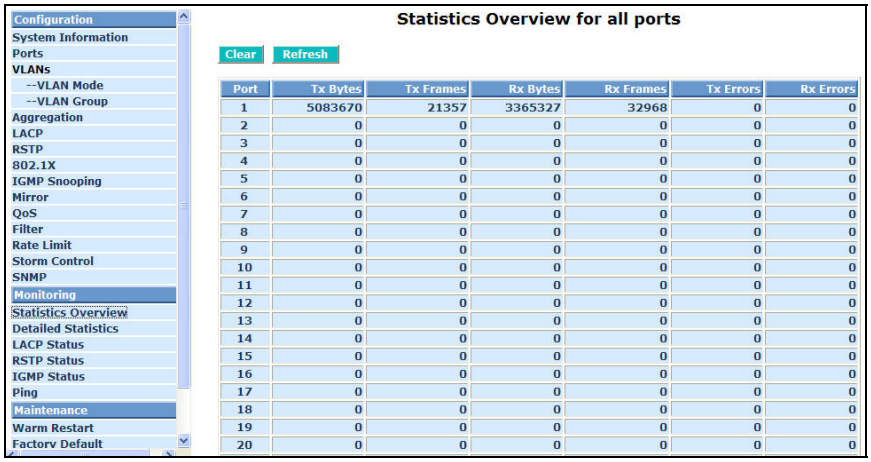
The counting number of the packet received.

Tx Errors:

Number of bad packets transmitted.

Rx Errors:

Number of bad packets received.



Port	Tx Bytes	Tx Frames	Rx Bytes	Rx Frames	Tx Errors	Rx Errors
1	5083670	21357	3365327	32968	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0
11	0	0	0	0	0	0
12	0	0	0	0	0	0
13	0	0	0	0	0	0
14	0	0	0	0	0	0
15	0	0	0	0	0	0
16	0	0	0	0	0	0
17	0	0	0	0	0	0
18	0	0	0	0	0	0
19	0	0	0	0	0	0
20	0	0	0	0	0	0

Fig. 4-28 Statistics Overview for all ports

4-3-2. Detailed Statistics

Function name:

Detailed Statistics

Function description:

Display the detailed counting number of each port's traffic. In the Fig. 4-26, the window can show all counter information each port at one time.

Parameter description:

Rx Packets:

The counting number of the packet received.

RX Octets:

Total received bytes.

Rx High Priority Packets:

Number of Rx packets classified as high priority.

Rx Low Priority Packets:

Number of Rx packets classified as low priority.

Rx Broadcast:

Show the counting number of the received broadcast packet.

Rx Multicast:

Show the counting number of the received multicast packet.

Rx Broad- and Multicast:

Show the counting number of the received broadcast with multicast packet.

Rx Error Packets:

Show the counting number of the received error packets.

Tx Packets:

The counting number of the packet transmitted.

TX Octets:

Total transmitted bytes.

Tx High Priority Packets:

Number of Tx packets classified as high priority.

Tx Low Priority Packets:

Number of Tx packets classified as low priority.

Tx Broadcast:

Show the counting number of the transmitted broadcast packet.

Tx Multicast:

Show the counting number of the transmitted multicast packet.

Tx Broad- and Multicast:

Show the counting number of the transmitted broadcast with multicast packet.

Tx Error Packets:

Show the counting number of the received error packets.

Rx 64 Bytes:

Number of 64-byte frames in good and bad packets received.

Rx 65-127 Bytes:

Number of 65 ~ 126-byte frames in good and bad packets received.

Rx 128-255 Bytes:

Number of 127 ~ 255-byte frames in good and bad packets received.

Rx 256-511 Bytes:

Number of 256 ~ 511-byte frames in good and bad packets received.

Rx 512-1023 Bytes:

Number of 512 ~ 1023-byte frames in good and bad packets received.

Rx 1024-Bytes:

Number of 1024-max_length-byte frames in good and bad packets received.

Tx 64 Bytes:

Number of 64-byte frames in good and bad packets transmitted.

Tx 65-127 Bytes:

Number of 65 ~ 126-byte frames in good and bad packets transmitted.

Tx 128-255 Bytes:

Number of 127 ~ 255-byte frames in good and bad packets transmitted.

Tx 256-511 Bytes:

Number of 256 ~ 511-byte frames in good and bad packets transmitted.

Tx 512-1023 Bytes:

Number of 512 ~ 1023-byte frames in good and bad packets transmitted.

Tx 1024-Bytes:

Number of 1024-max_length-byte frames in good and bad packets transmitted.

Rx CRC/Alignment:

Number of Alignment errors and CRC error packets received.

Rx Undersize:

Number of short frames (<64 Bytes) with valid CRC.

Rx Oversize:

Number of long frames(according to max_length register) with valid CRC.

Rx Fragments:

Number of short frames (< 64 bytes) with invalid CRC.

Rx Jabber:

Number of long frames(according tomax_length register) with invalid CRC.

Rx Drops:

Frames dropped due to lack of receiving buffer.

Tx Collisions:

Number of collisions transmitting frames experienced.

Tx Drops:

Number of frames dropped due to excessive collision, late collision, or frame aging.

Tx Overflow:

Number of frames dropped due to the lack of transmitting buffer.

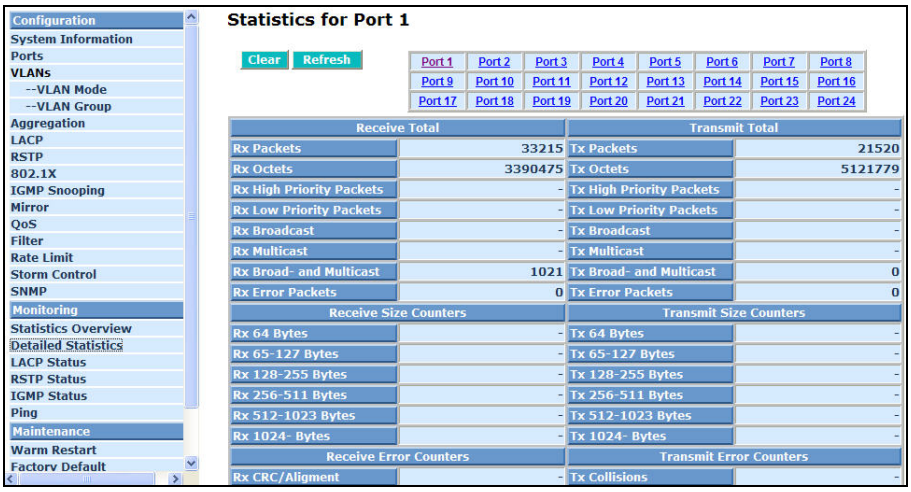


Fig. 4-29 Detailed Statistics for each port

4-3-3. LACP Status

Function name:

LACP Status

Function description:

Display the LACP status. In the Fig. 4-30, the window can show LACP information and status for each port at one time.

Parameter description:

LACP Aggregation Overview:

Show the group/port status. Red signs are set by default for link down ports; user are recommended to refer to the legend table below for detailed information.

LACP Port Status:

Group/Port:

Show the port number.

Normal : as Legend.

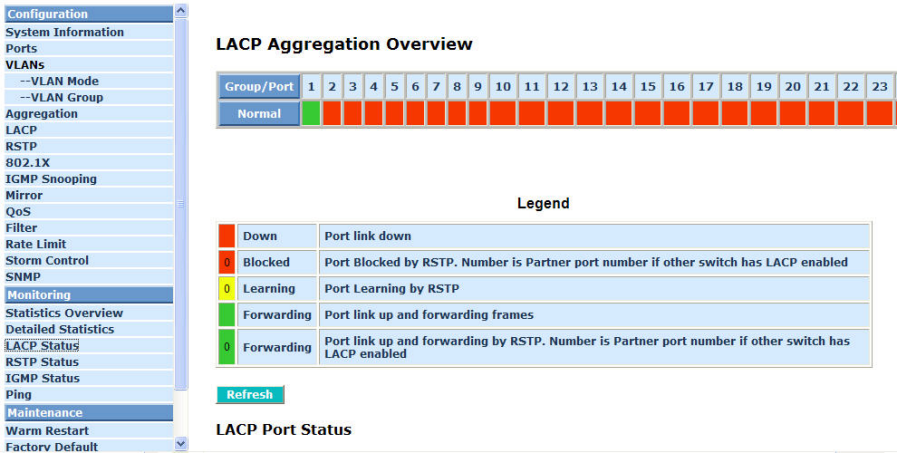


Fig. 4-30 LACP Status

4-3-4. RSTP Status

Function name:

RSTP Status

Function description:

Display the RSTP status. In the Fig. 4-28, the window can show the VLAN bridge information and statuses of 1~24 ports.

Parameter description:

RSTP VLAN Bridge Overview:

VLAN Id:

Show the VLAN Id.

Bridge Id:

Show this switch's current bridge priority setting and bridge ID which stands for the MAC address of this switch.

Hello Time:

Show the current hello time of the root bridge. Hello time is a time interval specified by root bridge, used to request all other bridges periodically sending hello message every "hello time" seconds to the bridge attached to its designated port.

Max Age:

Show the root bridge's current max age time.

Fwd Delay:

Show the root bridge's forward delay time.

Topology:

Show the root bridge's spanning tree topology.

Root Id:

Show root bridge ID of this network segment. If this switch is a root bridge, the "This switch is Root" will show this switch's bridge ID.

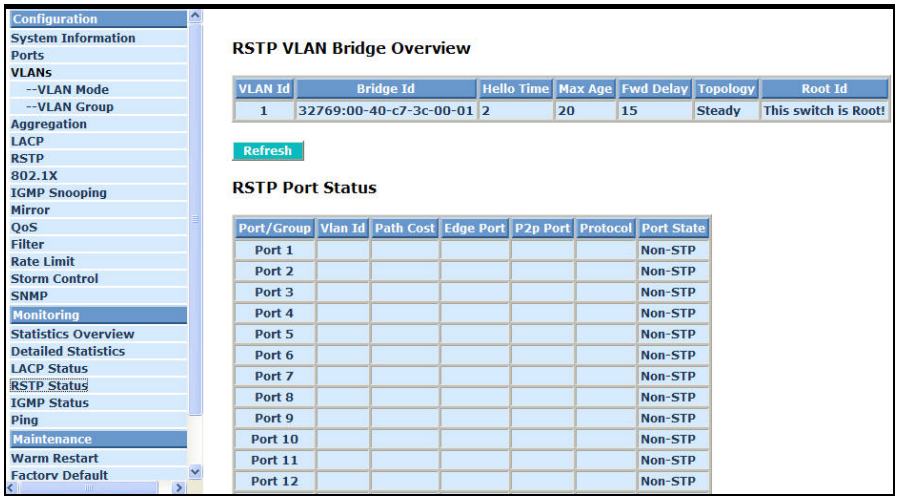


Fig. 4-31 RSTP Status

4-3-5. IGMP Status

Function name:

IGMP Status

Function description:

Display the IGMP status. In the Fig. 4-29, the window can show VLAN ID for each multicast group.

Parameter description:

VLAN Id:

Show VLAN Id for each multicast group.

Querier:

Show the group membership queries status.

Queries transmitted:

To count the group membership queries transmitted.

Queries received:

To count the group membership queries received.

V1 Reports:

When a host receives a group membership query, it identifies the groups associated with the query and determines to which groups it belongs. The host then sets a timer, with a value less than the *Max Response Time* field in the query, for each group it belongs. It calculates the number of times of IGMP V1 report.

V2 Reports:

When a host receives a group membership query, it identifies the groups associated with the query and determines to which groups it belongs. The host then sets a timer, with a value less than the *Max Response Time* field in the query, for each group it belongs. It calculates the number of times of IGMP V2 report.

V3 Reports:

When a host receives a group membership query, it identifies the groups associated with the query and determines to which groups it belongs. The host then sets a timer, with a value less than the *Max Response Time* field in the query, for each group it belongs. It calculates the number of times of IGMP V3 report.

V2 Leaves:

When a host leaves a group, it sends a leave group membership message to multicast routers on the network. It show the leaves number.

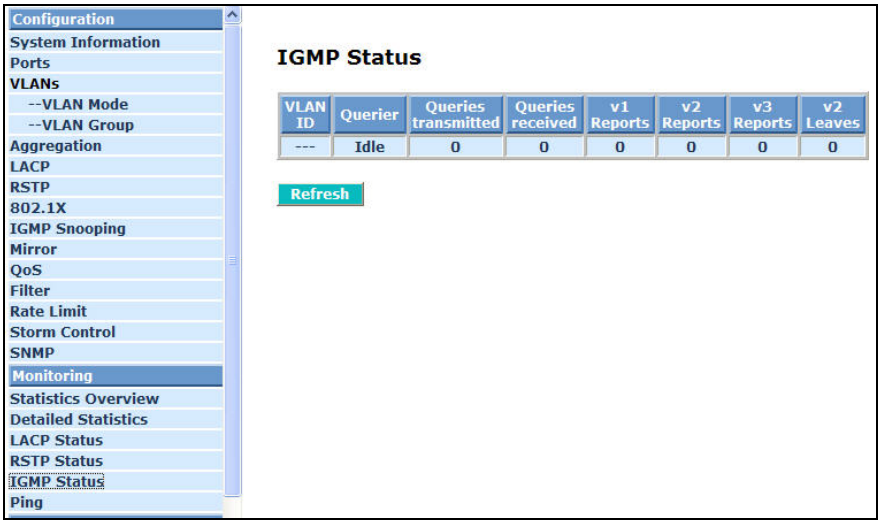


Fig. 4-32 IGMP Status

4-3-6. Ping Status

Function name:

Ping Status

Function description:

To setting up the target IP address for ping function of ICMP protocol and display the pinging status. In the Fig. 4-30, the window can show the pinging information.

Parameter description:

Ping Parameters:

Target IP address:

Set up a Target IP address to ping.

Count:

Use drop-down menu to set the number of echo requests to send. One of the four numbers can be chosen: 1, 5, 10 and 20.

Default: 1

Time Out (in secs):

Use drop-down menu to set the number of echo requests time out in seconds. One of the four numbers can be chosen: 1,5,10 and 20.

Default: 1

NOTE: Press **<Apply>** button to start up after you set up the parameters.

Ping Results:

Target IP address:

Show the active target IP address.

Status:

Show the result of the ping status.

Received replies:

Show the received replies in number of times.

Request timeouts:

Show the timeout of request.

Average Response time (In ms):

Show the average response time in milliseconds.

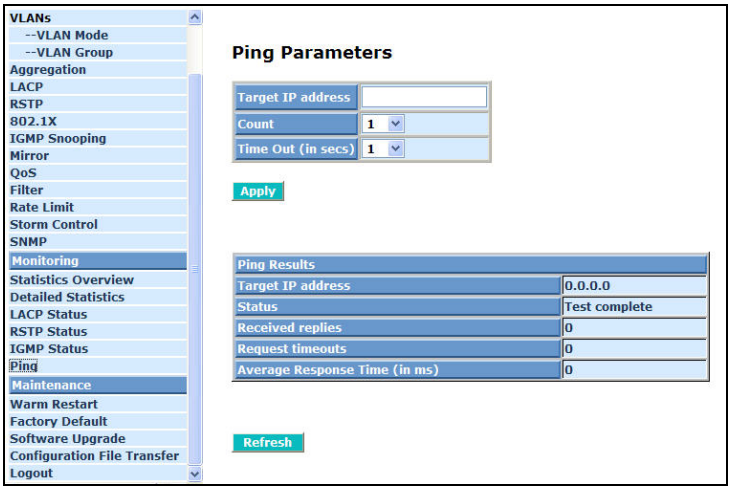
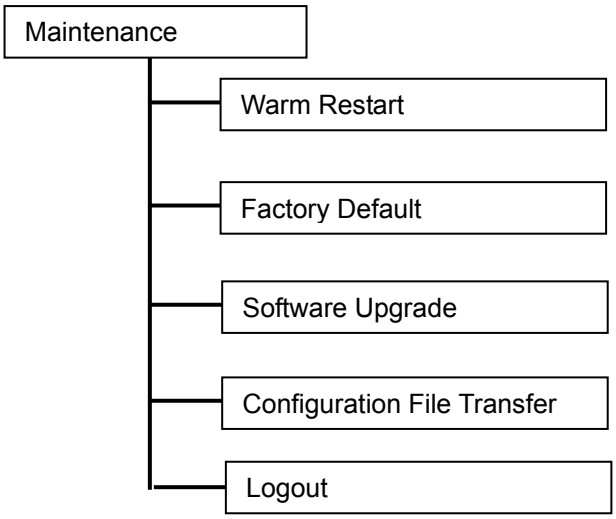

VLANs
--VLAN Mode
--VLAN Group
Aggregation
LACP
RSTP
802.1X
IGMP Snooping
Mirror
QoS
Filter
Rate Limit
Storm Control
SNMP
Monitoring
Statistics Overview
Detailed Statistics
LACP Status
RSTP Status
IGMP Status
Ping
Maintenance
Warm Restart
Factory Default
Software Upgrade
Configuration File Transfer
Logout
Ping Parameters
Target IP address
Count
1
Time Out (in secs)
1
Apply
Ping Results
Target IP address
0.0.0.0
Status
Test complete
Received replies
0
Request timeouts
0
Average Response Time (in ms)
0
Refresh

Fig. 4-33 Ping

4-4. Maintenance

There are five functions under the maintenance section.



4-4-1. Warm Restart

We offer you many ways to reboot the switch, toggle the power, hardware reset and software reset. You can press the RESET button in the front panel to reset the switch to its default setting. After upgrading software, you must reboot to have the new configuration taken effect. Here we will be discussing the software reset for the “reboot” in the main menu.

Function name:

Warm Restart

Function description:

Reboot the switch. Reboot takes the same effect as the RESET button on the front panel of the switch. Press **<Yes>** button to confirm a warm restart, and it will take around thirty (30) seconds to complete the system boot.

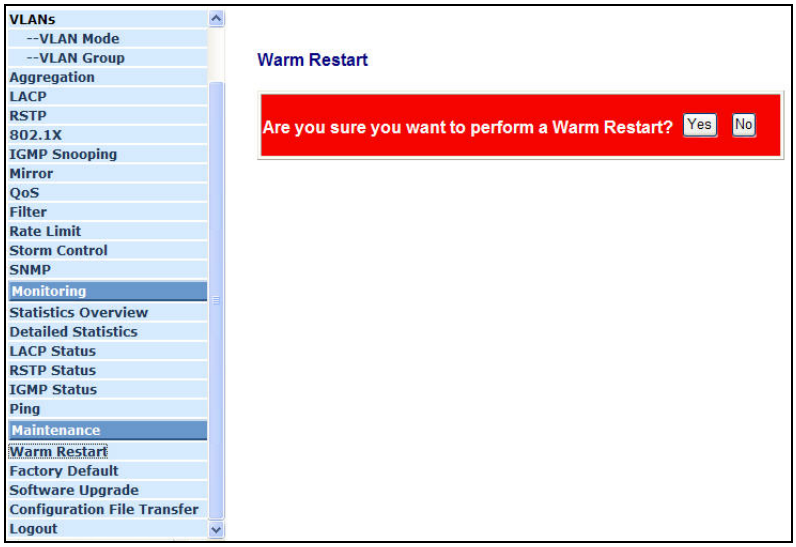


Fig. 4-34 Warm Restart

4-4-2. Factory Default

Function name:

Factory Default

Function description:

Factory Default provides the function to retrieve default settings and replace current configuration. Except the IP address setting, all settings will be restored to the factory default values when “Factory Default” function is performed. If you want to restore all configurations including the IP address setting to the factory default, please press the “RESET” button on the front panel.

Note for “RESET” button:

You must press the “RESET” button over 3 seconds to restore the factory default setting.

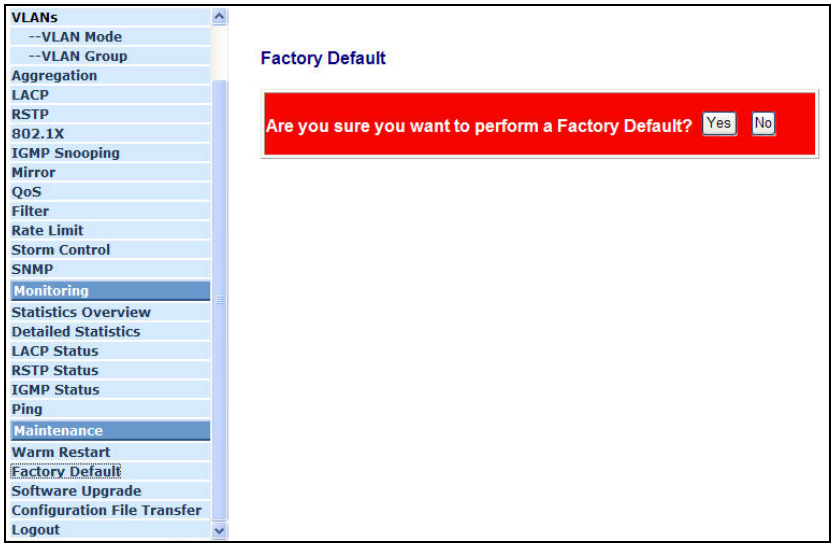


Fig. 4-35

4-4-3. Software Upgrade

Function name:

Software Upgrade

Function description:

Browse through your PC for a newer version of software pre-saved on your PC and upgrade the switch.

Fig. 4-36 Software Upgrade

4-4-4. Configuration File Transfer

Function name:

Configuration File Transfer

Function description:

Backup the switch's configuration file onto your computer to prevent accidental data lost. If a device configuration crash occurs, or to configure a new switch, this pre-saved configuration backup file can be used to quickly restore the switch back to its previous state, or save you time if you need to set a new switch with the same configuration.

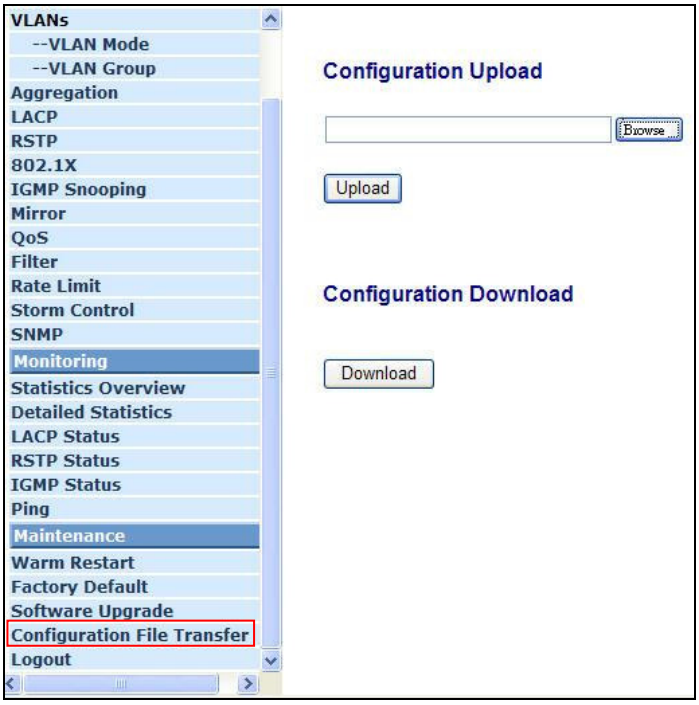


Fig. 4-37 Configuration Upload/Download

4-4-5. Logout

Besides the auto logout function as we mentioned in the system configuration section, the switch also allows the user to logout manually by performing Logout function.

Function name:

Logout

Function description:

The switch allows you to logout the system to prevent unwanted accesses by other users without permission. If you do not logout and exit the browser, the switch will automatically have you logged out. Besides this manually logout and implicit logout, you can set up the parameter of Auto Logout Timer in system configuration function to explicitly ON/OFF this logout function.

Parameter description:

Auto/Manual Logout:

If no action and no key stroke in any function screen for more than the minutes you set up in Auto Logout Timer, the switch will have you logged out automatically. Press the **<Logout>** button in Logout function to exit the system manually and immediately.

Fig. 4-38

5. Maintenance

5-1. Resolving No Link Condition

The possible causes for a no link LED status are as follows:

- The attached device is not powered on
- The cable may not be the correct type or is faulty
- The installed building premise cable is faulty
- The port may be faulty

5-2. Q&A

1. Computer A can connect to Computer B, but cannot connect to Computer C through the 24-Port GbE Web Smart Switch.
   - ✓ The network device of Computer C may fail to work. Please check the link/act status of Computer C on the LED indicator. Try another network device on this connection.
   - ✓ The network configuration for Computer C may be something wrong. Please verify the network configuration on Computer C.

2. The uplink connection function fails to work.
   - ✓ Please make sure that ports on the opposing device are connection ports. Please check if connection ports are used on that 24-Port GbE Web Smart Switch.
   - ✓ Please check the uplink setup of the 24-Port GbE Web Smart Switch to verify the uplink function is enabled.

3. There is no console interface seen to be built on the device.
   - ✓ 24-Port GbE Web Smart Switch has no console port, so you cannot use console interface to connect with 24-Port GbE Web Smart Switch.

4. How to configure the 24-Port GbE Web Smart Switch.

   - ✓ User can use an Internet browser such as IE in Window® series of computers to control the web smart functions of 24-Port GbE Web Smart Switch. First, choose any port on the 24-Port GbE Web Smart Switch. Then, use IE and type default IP address, 192.168.1.1, to connect to the 24-Port GbE Web Smart with RJ45 network cable. Finally, the login screen will appear at once.
   - ✓

Appendix A
Technical Specifications

Features

- 20 (10/100/1000Mbps) Gigabit Ethernet (TP) switching ports are compliant with IEEE802.3, 802.3u, 802.3z and 802.3ab.
- 4 Gigabit TP/SFP fiber are dual media ports with auto detected function.
- Non-blocking store-and-forward shared-memory Web-Smart switched.
- Supports auto-negotiation for configuring speed, duplex mode.
- Supports 802.3x flow control for full-duplex ports.
- Supports collision-based and carrier-based backpressure for half-duplex ports.
- Any ports can be in disable mode, force mode or auto-polling mode.
- Supports Head of Line (HOL) blocking prevention.
- Supports broadcast storm filtering.
- Web-based management provides the ability to completely manage the switch from any web browser.
- Supports Port-based VLAN and Tag-based (IEEE802.1Q) VLAN.
- Auto-aging with programmable inter-age time.
- Supports 802.1p Class of Service with 2-level priority queuing.
- Supports port trunking with flexible load distribution and failover function.
- Supports port sniffer function
- Programmable maximum Ethernet frame length of range from 1518 to 9600 bytes jumbo frame.
- Supports port-based VLAN, 802.1Q tag-based VLAN.
- Efficient self-learning and address recognition mechanism enables forwarding rate at wire speed.

Hardware Specifications

- **Standard Compliance:** IEEE802.3/802.3ab / 802.3z / 802.3u / 802.3x
- **Network Interface:**

Configuration	Mode	Connector	Port
10/100/1000Mbps Gigabit TP	NWay	TP (RJ-45)	1 - 24
1000Base-SX Gigabit Fiber	1000 FDX	*SFP	21,22,23,24 (Option)
1000Base-LX Gigabit Fiber	1000 FDX	*SFP	21,22,23,24 (Option)
1000Base-LX Single Fiber WDM (BiDi)	1000 FDX	*SFP	21,22,23,24 (Option)

*Port 21,22,23, 24 are TP/SFP fiber dual media ports with auto detected function
*Optional SFP module supports LC or BiDi SC transceiver

- **Transmission Mode:** 10/100Mbps support full or half duplex
  1000Mbps support full duplex only
- **Transmission Speed:** 10/100/1000Mbps for TP
  1000Mbps for Fiber
- **Full Forwarding/Filtering Packet Rate:** PPS (packets per second)

Forwarding Rate	Speed
1,488,000PPS	1000Mbps
148,800PPS	100Mbps
14,880PPS	10Mbps

- **MAC Address and Self-learning:** 8K MAC address
- **Buffer Memory:** Embedded 400 KB frame buffer
- **Flow Control:** IEEE802.3x compliant for full duplex
  Backpressure flow control for half duplex
- **Cable and Maximum Length:**

TP	Cat. 5 UTP cable, up to 100m
1000Base-SX	Up to 220/275/500/550m, which depends on Multi-Mode Fiber type
1000Base-LX	Single-Mode Fiber, up to10/30/50Km
1000Base-LX WDM (BiDi)	Single-Mode Single Fiber, up to 20Km

- **Diagnostic LED:**

  System LED : Power
  Per Port LED:
  10/100/1000M TP Port 1 to 24 : LINK/ACT, 10/100/1000Mbps
  1000M SFP Fiber Port 21,22,23,24 : SFP(LINK/ACT)

- **Power Requirement** **:** AC Line

  Voltage : 100~240 V
  Frequency : 50~60 Hz
  Consumption : 30W
- **Ambient Temperature** **:** 0° to 50°C
- **Humidity** **:** 5% to 90%
- **Dimensions** **:** 44(H) × 442(W) × 209(D) mm
- **Comply with FCC Part 15 Class A & CE Mark Approval**

Management Software Specifications

System Configuration	Auto-negotiation support on 10/100Base-TX ports, Web browser can set transmission speed (10/100Mbps) and operation mode (Full/Half duplex) on each port, enable/disable any port, set VLAN group, set Trunk Connection.
VLAN Function	Port-Base / 802.1Q-Tagged, allowed up to 24 active VLANs in one switch.
Trunk Function	Ports trunk connections allowed
Bandwidth Control	Supports by-port Egress/Ingress rate control
Quality of Service (QoS)	Referred as Class of Service (CoS) by the IEEE 802.1P standard Two queues per port
Network Management	Web browser support based on HTTP Server

Note: Any specification is subject to change without notice.

Appendix B
MIB Specifications

MIB II Enterprise MIB brief description is listed as below.

```
PRIVATE-ES-5240G+-MIB DEFINITIONS ::= BEGIN

IMPORTS
   mib-2, DisplayString,ifIndex                          FROM RFC1213-MIB
   enterprises,Counter, TimeTicks, Gauge,IpAddress       FROM RFC1155-SMI
   OBJECT-TYPE                                           FROM RFC-1212
   TRAP-TYPE                                             FROM RFC-1215;

privatetech             OBJECT IDENTIFIER ::= { enterprises 5205 }

switch          OBJECT IDENTIFIER ::= { privatetech 2 }

ES-5240G+ProductId        OBJECT IDENTIFIER ::= { switch 7 }

ES-5240G+Produces         OBJECT IDENTIFIER ::= { ES-5240G+ProductId 1 }

ES-5240G+IllegalLogin  TRAP-TYPE
          ENTERPRISE ES-5240G+ProductId
          DESCRIPTION
         "Send this trap when the illegal user try to login the Web management UI. "
          ::= 1

ES-5240G+RxErrorThreshold  TRAP-TYPE
          ENTERPRISE ES-5240G+ProductId
          VARIABLES   { ifIndex }
          DESCRIPTION
         "Send this trap when the number of the Rx bad packet over the Rx Error
          Threshold. The OID value means the port number. "
          ::= 2

ES-5240G+TxErrorThreshold  TRAP-TYPE
          ENTERPRISE ES-5240G+ProductId
          VARIABLES   { ifIndex }
          DESCRIPTION
         "Send this trap when the number of the Tx bad packet over the Tx Error
Threshold.
          The OID value means the port number. "
          ::= 3
END
```